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

[Attached to the *SEC Office Notification No. Nor Por. 7/2565*]

Scope of Operation:

1. High-risk business operators shall comply with all clauses hereof.
2. Low-risk or medium-risk business operators shall comply with all clauses, except the clauses where the term "*[High-risk]*"is specified.
3. Small-scale business operators shall comply with the fundamental guidelines at least in the following matters:

Table of Content

Chapter 1 Information Technology Governance

Provisions in Appendix 2 **Attached to the *Notification No. Sor. Thor. 38/2565***	**Guidelines**
1.1 Roles and Responsibilities of the Board of Directors	
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. A business operator should establish an IT governance framework with the following details: (1) structure of governance, roles, and responsibilities of the board of directors, executives, and relevant units; and (2) processes related to IT governance, such as - preparation and application for approval of IT plans - preparation of IT resource plan and management of IT resources, and - monitoring and reporting of IT performance. 2. A business operator should establish an annual IT plan to ensure that IT use will be in line with business operation strategies.
1.2 allocation of appropriate and sufficient IT resources and IT personnel for business operation;	1. A business operator should allocate IT resources and IT personnel in line with goals according to established missions, strategies, policies, and operational plans.

Provisions in Appendix 2 Attached to the *Notification No. Sor. Thor. 38/2565*	Guidelines
1.3 stipulation of written policies related to IT risk supervision, which shall at least cover the policies prescribed in Clause 2.2 in Part 2;	[No specific guidelines have been prescribed.]
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;	[No specific guidelines have been prescribed.]
1.5 creation of knowledge and awareness of IT risk for directors and personnel continuously and effectively; and	[No specific guidelines have been prescribed.]
1.6 monitoring, reviewing, and reporting on the conformance of the policies in Clause 1.3 to the board of directors of the business operator at least once a year. **In case of the occurrence of any event or change which may significantly affect the conformance of such policies, the board of directors shall be informed without delay.**	1. A business operator should establish a process for monitoring, reviewing, and overseeing the preparation of a report on the conformance of the policies related to IT risk supervision to ensure that the report can be prepared completely and accurately. 2. A business operator should require that the reporting on the conformance of the policies related to IT risk supervision to its board of directors will cover the following matters: (1) IT risk management results by the IT risk management unit or relevant unit; (2) overall results of conformance with rules, regulations or policies on IT security by the IT compliance unit or related unit; (3) IT audit findings and status of corrective actions by the IT audit unit or a relevant unit; (4) key IT performance such as: (a) significant IT incidents or problems; (b) IT capacity and system utilization; (c) overall progress of IT projects and significant projects;

Provisions in Appendix 2 Attached to the *Notification No. Sor. Thor. 38/2565*	Guidelines
	(d) IT operation of third parties, such as results of compliance with the service level agreement; and (e) results of IT contingency plan exercise, and activation of the plan (if any).
1.2 Structure of Governance	
Part 2 Organizational IT Risk Governance 2.1 A business operator shall establish an IT governance and management structure 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 (3 LoDs) concept, under which IT-related duties are clearly segregated as follows: 1st Line of Defense: Operations 2nd Line of Defense: Risk management and compliance of applicable laws and regulations; and 3rd Line of Defense: Audit	1. A business operator should establish an IT governance and management structure with checks and balances and with appropriate segregation of duties according to the three Lines of Defense (3 LoDs) concept as follows: (1) Operations (first line of defense) shall refer to the IT operation unit and IT system users for the performance of work; (a) the IT operation unit is tasked with the performance of work according to its responsibilities, assessment and control of IT risk, monitoring and reporting of IT operations to the board of directors or designated high-level executives; and (b) IT system users for the performance of work are obligated to comply with policies and regulations related to IT security, as well as having joint responsibility for the assessment and management of IT risk related to system usage. (2) Risk management and compliance of applicable laws and regulations related to IT operations (second line of defense) shall refer to the IT risk management unit and the IT compliance unit. (a) the IT risk management unit is responsible for establishing a policy framework and IT risk management processes, ensuring the risk assessment is in line with the established IT risk management framework, as well as providing advice, monitoring risk, and reviewing IT risk

Provisions in Appendix 2 Attached to the *Notification No. Sor. Thor. 38/2565*	Guidelines
	control to meet the risk appetite. The IT risk management unit is also responsible for collecting and establishing the connection between IT risk and other risks, as well as presenting risk management results to the IT risk oversight committee; and (b) the IT compliance unit is responsible for ensuring compliance with applicable laws and regulations, including monitoring, providing advice on and reviewing compliance with applicable laws and regulations. (3) IT audit (third line of defense) shall refer to the IT audit unit tasked with auditing the performance of work by the units acting as the first and second lines of defense units to ensure their compliance with applicable IT policies, standards, and laws. The units at this line of defense may be in-house auditors (internal auditors) or external auditors that are independent of the units acting as the first and second lines of defense. 2. *[High-risk] A business operator should have at least one member of the board of directors or one advisor of the business operator who has the IT knowledge or experience to enable its board of directors to set the direction and oversee that the business operator has used IT appropriately to its business strategies. The business operator may consider the qualifications of such director or advisor with the IT knowledge or experience based on the following matters where the business operator may include other criteria in its consideration as appropriate:* *(1) having graduated in IT or related fields; or* *(2) having experience as chief of the IT function or having responsibility as an executive related to IT or having experience in providing IT-related consultancy; or* *(3) having experience or having been appointed as a member of the committee or working group that is related to IT.*

Provisions in Appendix 2 Attached to the *Notification No. Sor. Thor. 38/2565*	Guidelines
	If the board of directors of the business operator has appointed a sub-committee to provide IT advice to the board, the business operator should clearly prescribe the roles and duties of the sub-committee in writing. The sub-committee should consist of at least one member with IT knowledge or experience. 3. *[High-risk] A business operator should appoint at least one chief information security officer (CISO) or executive responsible for IT security management who should have at least the following qualifications, extent of authority and duties:* *(1) being independent of the IT operations function and IT development function to be in line with checks and balances;* *(2) being a person equipped with the knowledge of or experience in IT and IT security management;* *(3) having sufficient authority to perform duties efficiently and effectively by being able to perform at least the following acts:* *(a) reporting significant problems or incidents affecting IT security to the organization's top management and the committee directly related thereto; and* *(b) providing opinions on cyber security threats and IT security risk management to the business operator's board of directors or the committee that is related to IT operations management and governance such as the IT steering committee or IT risk committee, and jointly making decisions on undertaking acts regarding IT security and cyber security threats with significant impacts.* 4. *[High-risk] The board of directors of the business operator <u>may</u> appoint a committee to perform duties related to IT risk governance, such as:* *(1) IT management and IT operations oversight committee (such as the IT steering committee or the designated committee) to ensure the establishment of IT strategies, policies and plans are in*

Provisions in Appendix 2 Attached to the *Notification No. Sor. Thor. 38/2565*	Guidelines
	conformity with the business operator's business strategies; *(2) IT risk management committee (such as the risk management committee or the assigned committee) to ensure the establishment of an IT risk management policy, supervising and monitoring IT operations to ensure its compliance with the established policies, including ensuring compliance with applicable laws and regulations related to IT.* *(3) IT audit committee (such as the audit committee or the assigned committee) to enable the business operator to have independent IT audit, covering IT operations, IT risk management and compliance with applicable laws and regulations related to IT.*
1.3 Policies on IT Risk Supervision	
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 such board of directors as follows:	
2.2.1 IT Risk Management Policy shall cover the following matters: (1) roles and responsibilities of persons involved in IT risk management; and (2) establishment of an IT risk management process to ensure the risk will be in line with the organization's risk appetite.	The IT risk management procedure should cover the followings: 1. The risk criteria should include the likelihood or frequency of risk scenarios and the significance or potential impacts, in order to prioritize the risk in risk management. 2. The IT risk appetite should be considered by the risk management committee (if any) and approved by the business operator's board of directors. The IT risk appetite should be in line with the enterprise risk management (if any). 3. Risk assessment should be conducted at least once a year and upon any significant change to the IT system. The procedure should at least cover the following matters: (1) Risk identification

Provisions in Appendix 2 Attached to the *Notification No. Sor. Thor. 38/2565*	Guidelines
	Identification of IT risk scenarios that may occur or that have already occurred to the business operator or other persons using similar technology, including cyber security threats and vulnerabilities affecting business operations, should be provided. Such risk scenarios may be caused by internal factors, such as operational procedures, application system, or personnel, as well as other external factors, such as compliance with laws, service usage, system connection or data access by third parties. (2) Risk analysis IT risk analysis should be conducted to set out appropriate risk management practices, which should at least cover the following acts: (a) designating a responsible person for risks or risk owner; (b) specifying the existing controls; and (c) analyzing the likelihood or frequency of risk scenarios and significance or potential impacts of such scenarios. (3) Risk evaluation Risk evaluation should be conducted to appropriately prioritize risk management, which should at least include the following acts: (a) assessing the outcome obtained from risk analysis, namely the likelihood and potential impact and the established risk criteria to identify the risk level of each IT risk scenario; and (b) prioritizing IT risks. 4. *[High-risk] A business operator should conduct IT risk assessment to keep pace with the change in the company risk profile which may be caused by both internal and external factors, such as issuance of*

Provisions in Appendix 2 Attached to the *Notification No. Sor. Thor. 38/2565*	Guidelines
	new products, changing of IT standards and requirements in the industry, or detection or indication of new technological risks. 5. For risk treatment, a business operator should establish IT risk treatment options that are appropriate and in line with risk assessment result to ensure that the residual risk will meet the risk appetite, which should at least include the following acts: (1) establishment of guidelines on risk treatment by taking into account the cost-effectiveness and appropriate methods for the business operator, such as risk avoidance, risk mitigation, risk transference and risk acceptance by presenting reasons to executives for decisions; (2) prescription of details of tasks that must be performed, the responsible person, and duration for operations; (3) assessment of whether the level of residual risk remains within the risk appetite; (4) application for approval for a risk management plan from the board of directors or the assigned high-level executive; (5) communication of the risk management plan to related persons 6. Preparation of a risk register: A risk register should be prepared to record the risk assessment results and guidelines on risk treatment. Examples of details are as follows: (1) date of risk assessment; (2) details of risk scenarios; (3) likelihood or frequency of risk scenarios; (4) significance or potential impacts; (5) inherent risk; (6) guidelines on risk treatment;

Provisions in Appendix 2 Attached to the *Notification No. Sor. Thor. 38/2565*	Guidelines
	(7) risk owner; (8) residual risk; and (9) status of risk treatment. 7. Risk monitoring and review: An IT risk monitoring and review process should be established and should cover the following acts: (1) designation of the responsible person for risk monitoring and review; (2) establishment of key IT risk indicators to enable efficient risk trends monitoring and the review of risk control measures; and (3) monitoring of the progress of operations under the IT risk management plan. 8. Risk reporting: IT risk assessment outcome and IT risk management outcome should be reported at least once a year to the business operator's board of directors.
2.2.2 IT Security Policy shall address the following matters: (1) organization of information technology security; (2) personnel management and third-party management; (3) IT asset management; (4) data security; (5) access control; (6) cryptographic control; (7) physical and environmental security;	[No specific guidelines have been prescribed.]

Provisions in Appendix 2 Attached to the *Notification No. Sor. Thor. 38/2565*	Guidelines
(8) IT operations security; (9) communication system security; (10) IT project management, system acquisition, development, and maintenance; (11) IT incident management; and (12) IT contingency plan.	
2.3 A business operator shall put in place operations under 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 and responsibilities, and data access rights in an easily accessible manner to enable such related persons to understand and comply with the policies properly.	1. In communicating the policies to third parties, a business operator should consider details that the third parties should know in order to be able to perform work in line with the business operator's policies, also taking into account confidentiality.
2.3.2 Establishment of operational processes and procedures in compliance with the policies under Clause 2.2.	1. A business operator should establish IT operation processes in writing to enable IT operation officers to perform their work correctly and in line with the policies related to IT risk governance. 2. A business operator should establish a procedure for granting approval for exception where there is necessary cause preventing compliance with the processes and procedures established by the business operator. Risk assessment and compensating control should be provided adequately and exception

[1] "Related persons" refer to personnel and directors, including third parties.

Provisions in Appendix 2 Attached to the *Notification No. Sor. Thor. 38/2565*	Guidelines
	approval should be sought from the authorized person prior to further action. The evidence of exception approval should also be documented. 3. A business operator should arrange for a review of the approved exceptions and their compensating controls at least once a year to ensure that they are still appropriate for the risks that may change in accordance with the business environment and the usage of information technology in business operations.
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.	[No specific guidelines have been prescribed.]
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 which may significantly affect IT risk governance and management.	[No specific guidelines have been prescribed.]

Chapter 2 Information Technology Security

Provisions in Appendix 3 Attached to the *Notification No. Sor. Thor. 38/2565*	**Guidelines**
2.1 Organization of Information Technology Security	
Part 1 Organization of Information Technology Security A business operator shall ensure there is such organization which shall at least contain the following features:	
1.1 establishing an organizational structure for IT operations with details of duties and responsibilities of the personnel in writing; and	[No specific guidelines have been prescribed.]
1.2 establishing a cross-check for IT operations to prevent potential risks;	1. A business operator should put in place clear segregation of duties in the performance of different tasks related to IT security to enable cross-check to reduce errors in its operation and reduce the opportunity for committing fraud, such as separating developers from the persons who deploy the system into the production environment. If no segregation of duties and responsibilities can be made due to restrictions on the scale of business or personnel, a business operator should establish compensating control measures instead, such as establishing a process for close and regular monitoring and inspecting performance of work of related personnel.
2.2 Personnel and Third-Party Management	
Part 2 Personnel and Third-Party Management	
2.2.1 Personnel Management	
Personnel subject to management	

Provisions in Appendix 3 Attached to the *Notification No. Sor. Thor. 38/2565*	Guidelines
2.1 Related personnel or those who use IT systems to perform their work.	
Management A business operator shall conduct personnel management under Clause 2.1 appropriately by at least undertaking the following acts: (1) having a process for personnel selection as follows: (1.1) considering knowledge, competence, and adequacy in the operation; and (1.2) checking background of personnel prior to employment sufficiently and in line with the risk of the position and duties and responsibilities thereof.	[No specific guidelines have been prescribed.]

Provisions in Appendix 3 Attached to the *Notification No. Sor. Thor. 38/2565*	Guidelines
(2) requiring the personnel to understand, acknowledge and affix their signature for acknowledgement of the following matters: (2.1) the roles and responsibilities of such personnel in relation to IT security; and (2.2) non-disclosure agreement;	1. A business operator should ensure that the personnel being employed have understood, acknowledged and affixed their signature to accept its employment conditions or organizational regulations, IT security policy, and non-disclosure agreement before they start working. 2. A non-disclosure agreement should, at a minimum, contain the following details: (a) ownership of sensitive business data, intellectual property, and prevention of data leakage; (b) responsibility for confidentiality and not disclosing data without permission; (c) warning and reporting to related persons if any data leakage or unauthorized disclosure is found; and (d) action that will be undertaken if the agreement is violated or cancelled, including requirements regarding the return or disposal of sensitive data upon the end of the agreement.
(3) raising awareness of IT risk among personnel who can access data or application systems within the organization so the personnel could use the application systems safely;	1. A business operator should promote and develop IT knowledge for its personnel regularly, such as organizing in-house training or arranging for the personnel to join external training, in order to ensure that the personnel will have the knowledge and understanding of secure and correct IT usage and to reduce potential risk. Such training should cover, for example, the following content: (a) IT security; (b) IT risk and cyber threats; and (c) applicable IT-related rules and laws. 2. A business operator should review the IT training program at least once a year to ensure that the content and details of relevant training are still sufficient and appropriate for the current IT risk trend. 3. A business operator should arrange for promotion of awareness of IT security and IT risk on a regular basis for users who may access sensitive data of the business operator or data of clients, such as phishing testing, social engineering testing, and carry out a cyber drill in preparation for cyber attacks.

Provisions in Appendix 3 Attached to the *Notification No. Sor. Thor. 38/2565*	Guidelines
(4) requiring personnel to refrain from using the IT systems in such a manner that will cause damage to the capital market or that is illegal, or violates requirements or code of conduct established by the business operator (if any);	1. A business operator should establish an acceptable IT use policy with details covering the scope of responsibility of IT users, what users should do and should not do. 2. A business operator should communicate the acceptable IT use policy to users for their acknowledgement and require them to sign to accept such policy.
(5) establishing disciplinary action policy for responding to personnel violating or failing to comply with IT security policies and measures; and	[No specific guidelines have been prescribed.]
(6) establishing a procedure to be undertaken upon the end of employment or change in the position in order to prevent potential breach or damage to IT assets.	1. A business operator should establish a support process upon any change of the position or end of employment, such as return of property to the organization, updating of rights, cancellation of rights upon termination of duties and responsibilities, as well as informing the related persons of the change of rights, duties and responsibilities to related persons.
2.2.2 Third-Party Management	
<u>Personnel subject to management</u> 2.2 Third parties are subject to management if the business operator undertakes any of the following acts: 2.2.1 using IT services from third parties; 2.2.2 connecting its IT system to third parties; or	

Provisions in Appendix 3 Attached to the *Notification No. Sor. Thor. 38/2565*	Guidelines
2.2.3 allowing third parties to access business operator's sensitive data or client data.	
<u>Management</u> A business operator shall conduct third-party management under Clause 2.2.1, Clause 2.2.2 or Clause 2.2.3 as follows: (1) assess the risk from the use of services, connection, or access of data by third parties, including subcontractors of third parties (if any);	1. A business operator should assess the risks and impacts prior to (1) using IT services from third parties, (2) connecting the IT system to third parties, and (3) authorizing third parties to accessits sensitive data or client data, by taking into account the following risks: (1) risks related to applicable laws and regulations, both domestic and international, such as the law on computer-related crime, the law on personal data protection, the law on electronic transactions, and the EU General Data Protection Regulation (GDPR); (2) risks from the inadequacy of due care oversight and management of third parties, such as the inability to conduct audits on the third parties by business operator's appointed auditors (3) concentration risks, such as a business operator and companies under the same business group using services from only one third party; (4) risk from reliance on only one third party (third party/vendor locked in), which limits any changes in technology or service providers or limits bringing the system or data back into one's own operation; (5) IT risk and cyber threats, such as the system provided by a third party has been interrupted or the system of the third party has vulnerabilities causing data loss or leakage; and (6) subcontracting risk, such as a subcontractor performing low-quality work. 2. A business operator should establish the level of significance of each third party.

Provisions in Appendix 3 Attached to the *Notification No. Sor. Thor. 38/2565*	Guidelines
(2) establishing practices and criteria for selection of third parties;	1. A business operator should, in writing, establish clear processes and criteria for selection of third parties to ensure that the third parties will be able to provide services that meet the business operator's requirements. The decision regarding the use of services, connection, or data access from a third party that are risky or significant should be approved by the board of directors or the assigned high-level executive. 2. A business operator should assess the potential of a third party (due diligence) based on the risk and significant of the third party, by taking into account the following matters: (1) financial position, reputation, expertise, experience, and ability to provide services in the past; (2) risk management, internal control, internal audit, and performance monitoring; (3) IT security; (4) business continuity management and readiness for handling threats or incidents; (5) compliance with applicable laws and regulations, such as examination of documents or certificates from a third party in complying with applicable laws and regulations or conducting a criminal background check. (6) compliance with international IT standards, such as examination of documents of being certified in ISO 27001 standard. As for compliance with international standards, the business operator should consider whether the third -party had been certified for key systems or the system that the business operator uses, connects or accesses data or if the certification comprehensively covers the entire organization; (7) the use of open technology to allow systems or data to be used or connected to other systems (interoperability) and to reduce the restrictions on migration or change of technology, service providers, and partners, including restrictions on returning the systems or data to the business operator's own operation; (8) If the service is subcontracted to another supplier, the business operator should consider details of

Provisions in Appendix 3 Attached to the *Notification No. Sor. Thor. 38/2565*	Guidelines
	information technology security of such supplier as well; and (9) *[High-risk] A business operator should conduct quality and reliability assessment on third parties by taking into account the experience, quality of delivered services and works, including IT security standards related to the goods and services and prepare a list of trusted third parties/trusted vendors to be used as part of the criteria for selection of service providers in the future.*
(3) prescribing roles, duties, and responsibilities of the business operator and the third party clearly and in writing	1. A business operator should prepare a written contract or agreement on the use of services, connection or data access from a third party to ensure that the third party is responsible for maintaining the appropriate security level of the IT system, with the details in line with the risk and significance of the third party as follows: (1) scope of service, connection, and access to data from the third party; (2) roles, duties, and responsibilities of the third party and the business operator; (3) minimum standards for operations of the third party, such as IT system security, confidentiality of data and not using data for any purposes other than those specified in the service contract or agreement; (4) service level agreement (SLA) for the use of services provided by the third party; (5) monitoring and reporting of the third party's performance, covering notification of any significant changes or problems and reporting of irregular events in a timely manner; (6) the list of contact persons and channels in the case of IT system security-related problems and incidents; (7) disposal of data upon termination or cancellation of service, connection, and access to data from the third party; (8) conditions or rights of the business operator to change, terminate or cancel a contract or agreement with the third party, such as in the case that the third party breaches the contract or agreement; (9) provision of an IT contingency plan that conforms with the business operator's IT contingency plan; and

Provisions in Appendix 3 Attached to the *Notification No. Sor. Thor. 38/2565*	Guidelines
	(10) responsibility for damage caused by the third party, such as in the case that the service provision is not as specified in the SLA. If there is any restriction on specifying important details and conditions in the agreement or contract executed with the third party, the business operator should assess the risk and consider adequate and appropriate measures for risk control, including seeking approval for exception from the authorized person.
(4) as for the third party who is an IT service provider with the significance as per the outcome of the risk assessment in Clause 2.2 (1), the service agreement or contract shall specify the right for the business operator, the SEC Office, and external auditors appointed by the business operator or the SEC Office to audit the operation and internal control of such third party. If there is necessary cause preventing the business operator from specifying the right to audit pursuant to the first paragraph above in the agreement or contract, the business operator shall have assessment or monitoring measures that are prudent, adequate and in line with the risk and significance of the use of service, connection or data access;	1. A business operator should specify the right for the business operator, the SEC Office, and external auditors appointed by the business operator or the SEC Office, as part of the service agreement or contract, to audit IT operation and internal control of the significant third party providing IT services. If such right cannot be specified, the business operator should consider choosing a third party whose IT operation has been audited by independent auditors who meet international standards, such as audit results under the SSAE 18 (SOC 2 Type 2 Report) standards, or PCI-DSS Attestation of Compliance (AOC). Additionally, the business operator should consider the details of the audit results prepared by the external auditors appropriately.

Provisions in Appendix 3 Attached to the *Notification No. Sor. Thor. 38/2565*	Guidelines
(5) having a non-disclosure agreement for third parties or their subcontractors if such persons can access business operator's sensitive data or clients data;	1. The non-disclosure agreement should contain details covering the scope of responsibility for confidentiality, non-disclosure without authorization, reporting to the business operator upon detection of data leakage or unauthorized disclosure, and disposal of sensitive data upon termination of the agreement or contract.
(6) supervising, monitoring, and managing risks from the use of services, connection, or access to data from third parties which shall be consistent with the risk level and the level of significance of such third parties;	1. A business operator should supervise, monitor and manage risks from the use of services, connection or access to data from a third party, to ensure that they are in line with the risks and significance of the third party, which should at least cover the following acts: (1) assigning a person responsible for continuously monitoring the performance of the third party. The monitoring should take into account the scope, level of risk and significance of use of services, connection or access to data from the third party; (2) preparing a register of third parties to enable comprehensive and continuous risks management, monitoring, and inspection of operation of third parties, with details as follows: (a) names of third parties; (b) details of the use of services, connection, or access to data from the third parties; (c) the level of risk and significance of the third parties; and (d) start date and end date of the contract or agreement; (3) prescribing measures for regular control and monitoring of the third parties' right to access the business operator's information to ensure that such right is on the need-to-know basis; (4) requiring the third party to report any incidents occurring during the operation of any relevant work to the business operator in a timely manner; (5) assessing the performance or the outcome of the service provided by the third party, both in the aspect of

Provisions in Appendix 3 Attached to the *Notification No. Sor. Thor. 38/2565*	Guidelines
	service efficiency, IT security and compliance with applicable laws when considering renewing the contract or when the period specified by the business operator is reached; and (6) reviewing the qualifications of the third party regularly to ensure that the third party is still suitably qualified.
(7) maintaining IT security from the use of services, connection, or access to data from a third party to be in line with the business operator's IT security standards; and	1. A business operator should have measures to ensure that the use of services, connection, and access to data from a third party will maintain IT security in accordance with the three critical principles, i.e., confidentiality, integrity and availability of the system and data, and in line with the business operator's IT security policy and standards or relevant international standards, such as ISO/IEC 27001. These measures should be appropriate to the risk level and significance of the third party.
(8) being prepared to respond to any potential IT incidents with significant impacts to ensure continuity of services or business operations.	1. A business operator should have an incident response plan in the case of IT incidents of the third party, which affect the business operator's operation. The plan should cover incidents related to cyber security incidents and personal data breaches.
2.3 IT Asset Management	
Part 3 IT Asset Management A business operator shall ensure there will be IT asset management to be used for IT security operations in an appropriate, complete and up-to-date manner, as follows:	
3.1 developing an IT assets inventory including hardware, software, and hardware and software license;	1. A business operator should establish IT asset management regulations that include the development and maintenance of the asset inventory, cancellation, and recall of assets. 2. A business operator should develop and maintain a complete and up-to-date inventory of IT assets consisting of hardware and virtual machines, with details such as:

<table>
<tr><th>Provisions in Appendix 3
Attached to the Notification No. Sor. Thor. 38/2565</th><th>Guidelines</th></tr>
<tr><td></td><td>
(1) asset serial number
(2) type of hardware
(3) specifications, brands, and models
(4) operating system and version
(5) asset owner
(6) asset administrator
(7) location
(8) start date of use/installation date
(9) warranty end date or end date of use under the contract
(10) type of possession (purchased or leased)
<u>Example:</u>
<table>
<tr><th>Asset Serial No.</th><th>Type</th><th>Description</th><th>Operating system/ version</th><th>Asset owner</th><th>Asset administrator</th><th>Location</th><th>Start date</th><th>Warranty End Date</th><th>Possession</th></tr>
<tr><td>RT123456</td><td>Switch</td><td>Brand: CC
Model: 1000
48 ports</td><td>A-OS 1.0.2</td><td>IT Department</td><td>A Company</td><td>Office</td><td>1 Mar 21</td><td>1 Mar 24</td><td>Purchased</td></tr>
<tr><td>SV212224</td><td>Router</td><td>Brand: JP
Model: 3700</td><td>13.2B</td><td>IT Department</td><td>IT Department</td><td>Office</td><td>5 May 64</td><td>5 May 23</td><td>Leased</td></tr>
</table>
</td></tr>
</table>

Provisions in Appendix 3 Attached to the *Notification No. Sor. Thor. 38/2565*	Guidelines

		8 ports							

3. A business operator should develop and maintain a complete and up-to-date inventory of IT software assets, with details such as:

(1) asset serial number

(2) software name

(3) specifications/usage

(4) operating system and version

(5) internal function that owns the software

(6) software registration date

(7) end date of use of services

(8) referenced hardware asset serial number

Example:

Asset serial no.	Software name	Specifications/usage	Operating system and version	Internal function that owns the software	Software registration date	End date of use of services	Hardware serial no. (for reference)
SP123456	Sheet processor pro	Software for processing	10.2.3A	IT	1 May 21	1 Dec 26	SV123456

Provisions in Appendix 3 Attached to the *Notification No. Sor. Thor. 38/2565*	Guidelines
	<table><tr><td></td><td></td><td>sheets/Excel</td><td></td><td></td><td></td><td></td><td></td></tr></table> 4. A business operator should regularly update the inventory of IT assets to ensure that it is completed and up-to-dated at least once a year and upon every significant change to the IT system.
3.2 designating a person or unit to be responsible for each item of IT assets; and	1. A business operator should designate a person or unit to be responsible for the preparation and updating of the inventory of IT assets, including maintenance of IT assets regularly over the whole asset life cycle.
3.3 providing regular maintenance of IT assets.	1. A business operator should maintain IT assets to be in good condition for use and ready to support continuous business operation, including having a plan to accommodate IT assets approaching the end of their life (EOL) or end of support (EOS) from the manufacturer, in an appropriate and timely manner. In case the business operator needs to use EOL or EOS assets, the business operator should assess the risks and establish appropriate risk control measures.
2.4 Data Security	
Part 4 Data Security A business operator shall maintain data security to ensure its confidentiality, integrity, and availability. as follows:	
4.1 designation of a person or unit as a data owner	1. A business operator should designate a person or unit as a data owner to be responsible for defining data users and their rights to access and alter data; as well as creating guidelines on data security.

Provisions in Appendix 3 Attached to the *Notification No. Sor. Thor. 38/2565*	Guidelines
4.2 data classification and guidelines on data security that are in line with the data classification, covering the following data: 4.2.1 data at endpoint; 4.2.2 data in transit; and 4.2.3 data at rest;	1. A business operator should establish data classification criteria and data handling methods based on data classification levels which should cover the entire data life cycle, from the creation or acquisition of data, processing, storage, usage, to data disposal, as well as clearly labelling data classification levels. 2. A business operator should establish data security measures that are consistent with the data classification levels, by covering the following data: (1) data at endpoint; (2) data in transit; and (3) data at rest. 3. A business operator should arrange for data security for data on storage media (data at rest) by performing the following acts: (1) consider the risk of possible data degradation on storage media, including data restoration in the case of storing data over a long period of time; (2) store the data storage media in a place that is safe and secure and as advised by the manufacturer thereof (if any); and (3) establish security measures for physical media transfer.
4.3 establishment of guidelines for secure data input, data processing, and data disposal;	1. A business operator should prescribe regulations on data disposal which should cover the duties and responsibilities of data owners and any related units, as well as data disposal methods suitable for data classification levels. 2. A business operator should establish a process for controlling data disposal which covers application for approval from the data owner before undertaking the disposal process, control and review of disposal operation, and preparation of an inventory of disposal of sensitive data.

<table>
<tr><th>Provisions in Appendix 3
Attached to the Notification No. Sor. Thor. 38/2565</th><th>Guidelines</th></tr>
<tr><td>4.4 preparation of a complete and up-to-date data inventory</td><td>1. A business operator should develop and maintain a complete and up-to-date data inventory. Examples of details are as follows:
(1) data registration number;
(2) name of data or set of data;
(3) description and type of data
(4) data classification level and level of sensitivity of data
(5) data owner and data administrator
(6) storage location or server
<u>Example:</u>
<table>
<tr><th>Data registration number</th><th>Name of data/set of data</th><th>Description</th><th>Classification level</th><th>Data owner</th><th>Data administrator</th><th>Storage location</th></tr>
<tr><td>ABC-IT-001</td><td>IT security policy</td><td>IT policy</td><td>Internal</td><td>IT Department</td><td>IT Department</td><td>Intranet system</td></tr>
<tr><td>ABC-Data-002</td><td>Customer information</td><td>Client’s data, i.e., name, surname, and date of birth.</td><td>Confidential</td><td>Securities Operation Department</td><td>IT Department</td><td>- DB server 015
- DB backup 012</td></tr>
</table></td></tr>
<tr><td colspan="2">2.5 Access Control</td></tr>
<tr><td>Part 5 Access Control</td><td></td></tr>
</table>

Provisions in Appendix 3 Attached to the *Notification No. Sor. Thor. 38/2565*	Guidelines
A business operator shall ensure there is efficient access control to prevent the access and revision to systems or data by ineligible or unauthorized persons as follows:	
5.1 establishing guidelines on management of user accounts and access rights by reviewing the right appropriately and regularly in line with the duties and responsibilities, including having a process for removal of the right when such right is no longer needed.	1. The guidelines on user account management should at least cover the following matters: (1) the unit responsible for user account management; (2) procedures for user accounts provisioning where user accounts should be able to identify the users and shared accounts should be avoided; (3) limitation or avoidance of using default user accounts; (4) review of user accounts at least once a year; and (5) disabling or deletion of user accounts when (1) users are no longer employees and (2) there is no need to use such user accounts. 2. The guidelines on management of the right to access data and IT systems should at least cover the following matters: (1) the unit responsible for management of the data and IT system access rights; (2) procedures for applying for approval for the data and IT system access rights from the authorized person, such as the system owner or data owner; (3) procedures for updating user rights upon changes in their duties and responsibilities or position; (4) procedures for revocation of user rights by immediately revoking the rights when the users are no longer employees and such rights are no longer required for work; (5) segregation of roles and duties of persons related to allocation of rights, such as access request, access

Provisions in Appendix 3 Attached to the *Notification No. Sor. Thor. 38/2565*	Guidelines
	authorization, and access administration, to ensure conformity with checks and balances; (6) prescription of user rights based on a need-to-know basis, need-to-use basis, and segregation of duties; (7) preparation of an authorization matrix of users that is in line with their positions, duties, and responsibilities to be used as the guidelines on stipulation of rights correctly and appropriately; and (8) regular review of the access rights at least once a year by stipulating periods for the review of the right in conformity with risks and importance of the right.
5.2 establishing an authentication process that is suitable for the risk and prevents repudiation; and	1. A business operator should establish a user authentication process that is efficient and suitable for the risk of unauthorized system access and the risk from repudiation, which should at least cover the following acts: (1) stipulation of user authentication methods suitable for the risks; (2) if a temporary (first-time) password is automatically generated for a user, the password should be delivered to the user in a secure manner and the user should change their password immediately upon receipt thereof; (3) requiring users to set their passwords that are complex and difficult to guess, which should have at least eight characters and consist of numbers and letters; The business operator may consider increasing the complexity thereof by requiring that passwords must contain numbers, upper-case letters, lower-case letters and special characters (such as “#”); (4) limiting the number of invalid authentication attempts by incorrect passwords before applying an account-lockout mechanism or any equivalent method to prevent a brute force attack, provided that in practice users should not be allowed to make more than 10 consecutive invalid authentication attempts ; (5) requiring that users should set a password that is not the same with the most recent four passwords they used or not the same as any password that has been used in the year before;

Provisions in Appendix 3 Attached to the *Notification No. Sor. Thor. 38/2565*	Guidelines
	(6) setting the default to not display the password on the screen when being entered; (7) store passwords in protected form to prevent unauthorized access or revision, including not storing the passwords in the same folder as the folder storing application data; and (8) requiring that users should be responsible for their user accounts (user IDs) and security for their authenticators, such as passwords or one-time passwords, including their personal data which may be used to request changing the account data, to prevent the use thereof by a malicious person. 2. *[High-risk] A business operator should have an automatic system for detecting and alerting irregular or suspicious authentication attempts, such as logging in from several source computers or logging in from source computers with different geographic locations within a short period of time.*
5.3 stipulating measures for controlling, limiting, and monitoring privileged users (privileged user management) as follows: 5.3.1 requiring MFA when logging in and changing passwords for the operating systems and the database systems that are related to the critical IT system; 5.3.2 if a business operator has restrictions on MFA, it may use another equivalent method instead and shall conduct risk assessment and consider adequate risk control measures before applying for exception	[No specific guidelines have been prescribed.]

Provisions in Appendix 3 Attached to the *Notification No. Sor. Thor. 38/2565*	Guidelines
approval; and	
5.3.3 implementing strict control and monitoring of the use of privileged user accounts;	1. A business operator should ensure control and monitoring of privileged user accounts as follows: (1) overseeing the granting of rights by limiting the rights based on roles and duties and the need for use; (2) limiting the number of privileged user accounts to a minimum or as necessary; (3) having a process for requesting the use of a privileged user account and approval from the authorized person; (4) regularly reviewing the privileged user accounts at least once a year; (5) stipulating authentication policies or measures for privileged user accounts to be stricter than those of general user accounts; (6) maintaining an authentication log, an access log, and an activity log for privileged user accounts appropriately; (7) reviewing the authentication, access, and activity logs of privileged user accounts upon the end of use or conducting regular and periodic reviews suitable for the risk, at least once a year, to ensure that the right is used appropriately; and (8) having a tool or process preventing logging into privileged user accounts and enhancement of the level of user rights by unauthorized persons, such as using the privilege access management (PAM) tool and using a monitoring system to generate alerts upon any use of privileged accounts.
2.6 Cryptographic Control	
Part 6 Cryptographic Control A business operator shall ensure there is cryptographic control that is reliable and in line	

Provisions in Appendix 3 Attached to the *Notification No. Sor. Thor. 38/2565*	Guidelines
with international standards by stipulating a secure method for encryption and key management to ensure that the confidentiality, integrity and authenticity of data are appropriate and efficient, as follows:	
6.1 stipulating secure encryption method;	1. In establishing secure encryption methods, the business operator should undertake at least the following acts: (1) stipulating the responsibility of the related units or personnel; (2) stipulating cryptographic algorithms to be in line with international standards, to be secure and suitable for the level of data classification; and (3) establishing the periods for conducting the review of the cryptographic algorithms to ensure that the cryptographic algorithms in use are still sufficiently secure for data security.
6.2 establishing cryptographic key management by stipulating control measures for generating, installing, storing, backing up, revoking and destroying cryptographic keys;	1. Regarding the generation and installation of the cryptographic keys, the business operator should undertake at least the following acts: (1) ensuring there is a secure environment and process for generating the cryptographic keys, such as selecting a reliable certification authority and disposing of data that may remain after the completion of the encryption key generation to prevent unauthorized access or recovery of such key; (2) stipulating the right to access the cryptographic keys to be accessible by only authorized persons; (3) stipulating the length of the cryptographic keys that is sufficient to prevent decryption by malicious persons, such as brute-force attacks; and (4) exchanging the cryptographic keys through secure processes and channels. 2. Regarding the storage and backup of the cryptographic keys, the business operator should undertake at least the

Provisions in Appendix 3 Attached to the *Notification No. Sor. Thor. 38/2565*	Guidelines
	following acts: (1) providing physical and logical security for the storage of the cryptographic keys, such as using Hardware Security Module (HSM) or a similar tool; and (2) backing up or archiving the cryptographic keys with the same level of security as that for the master cryptographic keys. 3. Regarding revocation or destruction of the cryptographic keys, the business operator should undertake at least the following acts: (1) prescribing rules and guidelines on changing and revoking the cryptographic keys, such as if the cryptographic keys have expired or are not safe; and (2) stipulating processes for destruction of the keys to ensure that such keys may no longer be used. 4. The business operator should keep a log of important activities related to the cryptographic keys, such as the generation, backup, access or use, and revocation of the keys.
6.3 stipulating measures on control of the cryptographic keys provided by a third party which shall be examined to ensure that the generated cryptographic keys are not shared with other users; and	1. If a business operator is unable to generate the cryptographic keys by itself or needs to use the cryptographic keys provided by a third party, the business operator should ensure that those cryptographic keys are not shared with other service users and are secure, by taking into account the service conditions or details as follows: (1) types of cryptographic keys; (2) descriptions of the cryptographic key management systems and processes; and (3) instructions for the use, and control of data encryption and decryption.
6.4 stipulating an incident response process in the case of leakage of the cryptographic key.	1. A business operator should specify the activities that must be performed upon leakage of the cryptographic keys, such as contacting the agency and persons related to the set of data that uses such set of cryptographic keys, inspecting of the set of data at risk of leakage, and changing or revoking the cryptographic key.

Provisions in Appendix 3 Attached to the *Notification No. Sor. Thor. 38/2565*	Guidelines
2.7 Physical and Environmental Security	
Part 7 Physical and Environmental Security A business operator shall put in place physical and environmental security for IT assets, as well as the protection system, and maintenance processes for hardware and facilities related to IT in order to prevent damage to IT assets stored at the primary site, backup site, and the third-party colocation data center.	1. A business operator should design its data center and areas related to the critical IT system by considering risks from natural disasters and human threats, such as putting in place sturdy walls or fences and providing adequate space between the backup site and the primary site. 2. The business operator should put in place management of access rights to the data center and areas related to the critical IT system by undertaking at least the following acts: (1) granting access rights based on necessity; (2) approving the access rights by the authorized person; (3) updating/revoking the access rights immediately upon resignation or change in duties or responsibilities of an employee; and (4) regularly reviewing the access rights at least once a year. 3. The business operator should put in place an authentication mechanism for accessing the data center and areas related to the critical IT systems, such as the use of an access card door system and keeping the log of access activities. For high-risk areas, the business operator may consider using MFA, such as an access card and a personal identification number (PIN). 4. The business operator should have measures for controlling access to the data center and areas related to the critical IT systems for employees who do not have full-time duties or who have temporary access by obtaining approval from the authorized person, keeping a log of access activities, and closely monitoring and escorting of such persons throughout the duration of their performance of duties in such areas. 5. The business operator should provide security systems for the data center, such as a CCTV system, a fire alarm

Provisions in Appendix 3 Attached to the *Notification No. Sor. Thor. 38/2565*	Guidelines
	and extinguisher system, a voltage and current control system, an uninterrupted power supply system, and a temperature and humidity control system, as well as maintain such security systems in good condition on a regular basis. 6. The business operator should put in place response measures for failure of the data center's facilities, such as an electrical system, telecommunications system and air-conditioning system. 7. The business operator should store important IT equipment, such as servers and network devices, in a restricted and secure place. 8. The business operator should put in place measures to protect the cables and electricity wires of the data center from interruption, interference or damage and should have them maintained regularly. 9. The business operator should ensure proper maintenance of IT hardware assets to ensure their continued availability and integrity. 10. The business operator should separate the delivery and loading areas where unauthorized persons could enter the premises from the areas in which data processing is performed. 11. The business operator should ensure that IT hardware assets will not be removed from the premises without authorization. 12. Prior to the cancellation of use or disposal of IT hardware assets, such as hard disks, switches, firewalls, and routers, the business operator should store the assets in a secure area and ensure that sensitive data and configuration data have been deleted, migrated, destroyed, or that a factory reset has been performed by techniques that make the original data non-retrievable.
2.8 IT Operations Security	
Part 8 IT Operations Security	

Provisions in Appendix 3 Attached to the *Notification No. Sor. Thor. 38/2565*	Guidelines
A business operator shall put in place IT operations security measures to ensure that operations related to data processing will be correct and secure. Such measures shall address at least management of the matters as described below.	
2.8.1 System Configuration Management	
8 . 1 System configuration management by establishing processes for controlling system configurations and regularly reviewing the system configurations to ensure that they are correct and secure.	1. A business operator should establish and document security configuration standards or security baselines to be enforced for the operating systems, the database systems and network devices, by taking into account the following matters: (1) deleting or disabling default user accounts, or changing the default passwords; (2) enabling secure authentication mechanisms; (3) disabling unnecessary services, applications, and connection ports; (4) logging; and (5) updating of software or firmware versions. 2. A business operator should regularly review and update security configuration standards or security baselines. 3. A business operator should set the security configurations of the operating systems, database systems and network devices according to the established standards prior to using them. 4. A business operator should review the security configurations of the operating systems, database systems, and network devices on a regular basis and upon every change to such systems and devices to ensure compliance with the established standards.

Provisions in Appendix 3 Attached to the *Notification No. Sor. Thor. 38/2565*	Guidelines
2.8.2 Change Management	
8.2 Sufficiently-secure change management to ensure that changes will correctly and completely reach the specified objectives and that unauthorized change is prevented.	1. A business operator should establish a documented process for change management to control changes to the IT infrastructure, IT system and operational procedures which may affect security. 2. A business operator should prescribe criteria for classification of changes based on the level of importance or urgent need, and establish a procedure for each type of changes, such as: (1) standard changes which were generally approved; (2) normal changes which must obtain approval in accordance with the normal process; and (3) emergency changes. 3. A business operator should designate a committee or an executive in charge of approving each type of changes; 4. A business operator should segregate duties of persons involved in the change process to prevent any person from being able to perform duties from the beginning to the end of the change process, such as the person eligible to submit a request, the person authorized to grant approval for the change, and the person who may change the system. 5. A business operator should document change requests and change approvals as evidence that the changes have been considered by the data owners, system owners, or authorized persons according to the specified rights. The change requests should specify the reasons and necessities for the changes and their potential impacts. 6. A business operator should put in place a system or a register for the storage of change requests and relevant documents to be used for controlling the change operations from the start to the end of the process and which may be used for the purpose of monitoring and reviewing the operations. 7. Where the change affects the operations, a business operator should communicate the change to the related persons to enable correct operations.

Provisions in Appendix 3 Attached to the *Notification No. Sor. Thor. 38/2565*	Guidelines
	8. A business operator should establish a fallback procedure if there is any error from the change, such as archiving the version of the system before the change. 9. In the case of an emergency change, there should be a process for consideration of risks and impacts, including the application for approval from the executive assigned to make decisions in emergency cases. After the change, the relevant executives and the Change Advisory Board (CAB) should be promptly informed. 10. *[High-risk] A business operator should stipulate roles, duties and responsibilities of the Change Advisory Board (CAB), which should consist of executives from the IT functions, the business functions and the relevant user functions, to consider the reasons and necessities and assess the impact prior to granting approval for the change in order to prevent unauthorized changes and prevent potential impacts on relevant systems.* *In addition, there should be a post-implementation review to ensure that the change is consistent with the established objectives.*
2.8.3 Capacity Management	
8.3 . As for capacity management, there shall be measures and processes in place for managing capacity, monitoring system efficiency, and forecasting the use of IT resources in order to ensure that the current business operations are supported and the resource are allocated efficiently for future usage.	1. A business operator should establish standards and regulations for capacity management to assess and monitor the adequacy of its IT infrastructure which covers the computer systems, database systems, communications network systems and IT-related facilities. 2. A business operator should conduct forecasting of IT resources by taking into account the volume of transactions and number of clients in normal conditions and potential crises, in order to conduct capacity planning for both primary and backup systems. 3. A business operator should have processes or tools in place for monitoring indicators of use of IT resources (threshold and trigger), such as performance, latency, capacity, and the utilization volume, to allow relevant officers to be promptly aware of any problems and address them appropriately.

Provisions in Appendix 3 Attached to the *Notification No. Sor. Thor. 38/2565*	Guidelines
	4. A business operator should regularly prepare a report on the adequacy of IT resources and submit it to the assigned committee or the relevant high-level executives for acknowledgement, in order to ensure oversight of the availability and adequacy of the system to support continuous business service provision and to be able to consider ways to reduce risks in a timely manner.
2.8.4 Server and Endpoint Security	
8.4 Server and endpoint security is aimed at protecting such devices from being used as a channel for data leaks or unauthorized access to the IT systems.	1. A business operator should establish server and endpoint security measures to prevent and detect malware and cyber security threats, including: (1) having control and monitoring processes to prevent unauthorized software installation; (2) installing and regularly updating tools for prevention and detection of malware, such as anti-virus, anti-malware, and intrusion prevention systems; and (3) controlling the use or connection to removable media, such as establishing guidelines for the use of a universal serial bus (USB) hard drives or external hard disks. 2. A business operator should implement controls for unattended IT user equipment to ensure security, including: (1) ensuring that documents, equipment used in the operation, or media that store sensitive or confidential data are not left unattended on work desks or unsafe places (clear desk policy); and (2) ensuring computer screens will not display sensitive data while not in use (clear screen policy), such as setting session timeout or automatic lock screen options after a specified period of inactivity. 3. A business operator should establish security measures for the use of virtualization technology, including securing the hypervisor, host operating systems, and guest operating systems, as well as ensuring appropriate security for data generated by the virtualization technology, such as virtual machine images and snapshots. 4. *[High-risk] A business operator should install a system or tool for threat detection that can analyze irregular*

Provisions in Appendix 3 Attached to the *Notification No. Sor. Thor. 38/2565*	Guidelines
	behavior, detect threats and archive data and evidence to enable a timely response to cyber security threats, such as installing an endpoint detection and response (EDR) system or the host-based intrusion prevention system (HIPS). 5. *[High-risk] A business operator should establish a process or tool to prevent data leaks due to unauthorized data transmission through various channels, such as mobile devices or removable media, email, online conference programs, and online communication tools.* 6. *[High-risk] If servers and endpoint devices have a function to disable connection ports, all external connection ports (such as USB ports) that support connection to removable media should be turned off and only turned on only as necessary with approval from an authorized person.*
2.8.5 Stipulation of Teleworking, Mobile Device, and Bring Your Own Device (BYOD) Security Policy and Measures	
8.5 Stipulation of teleworking, mobile device, and bring your own device (BYOD) security policy and measures by taking into account the related risks and putting in place appropriate control measures.	1. In the case of teleworking to access the critical IT system, a business operator should establish security measures that are prudent, sufficient and suitable for the IT system and the data being accessed. These measures should at least cover the following matters: (1) physical security measures that are sufficiently prudent for the scope of operations in the teleworking site; (2) granting of approval for teleworking by the authorized person or relevant executive; (3) stipulation of the access rights to data and the IT system via an external network as necessary only, including conducting regular reviews of such rights; (4) authentication of staff who operate through teleworking by prudent and secure means, such as using the multi-factor authentication (MFA) mechanism and logging in only through approved devices; (5) measures preventing the risk from devices used in teleworking as a channel to spread malware and data leakage;

Provisions in Appendix 3 Attached to the *Notification No. Sor. Thor. 38/2565*	Guidelines
	(6) measures protecting confidential or sensitive data, such as authentication before using a device (lock screen), encryption of data on devices used in the operation, or remote wipe-out. 2. Regarding the operations where mobile devices are used to access the critical IT system, the business operator should establish security measures that are prudently sufficient for the accessed IT system and data. These measures should at least cover the following matters: (1) registration of mobile devices before their use and conducting reviews of such registration at least once a year and upon replacement of devices to ensure that such mobile devices are sufficiently secure and safe. The business operator may use any other registration systems or technologies instead if deemed appropriate; (2) measures for the protection of confidential and sensitive data, such as authentication before using a device (lock screen), encryption of data on devices used in the operations or remote wipe-out; and (3) *[High-risk] provision of mobile device management tools with the capacity for management of security patches, device configuration, and management of virus and malware prevention.* 3. If employees are allowed to use their own devices (bring your own device: BYOD), the business operator should consider the relevant risks and establish appropriate risk control measures. These measures should at least cover the following matters: (1) establishment of criteria for approval of BYOD; (2) control of BYOD by allowing access to the communication systems, data, and IT systems as necessary only; (3) authentication to unlock access to BYOD, such as the use of passwords and fingerprint scanning; (4) If personal computers or notebooks of employees can be connected to the organization's internal network system or sensitive data, such devices should be installed with anti-virus/anti-malware programs which

Provisions in Appendix 3 Attached to the *Notification No. Sor. Thor. 38/2565*	Guidelines
	should be regularly updated; and (5) prohibition of the use of tablets and smartphones that have been rooted or jailbroken from accessing the IT systems. 4. *[High-risk] If employees are allowed to use their own device (bring your own device: BYOD), the business operator should put in place a process or a tool for inspecting, analyzing and monitoring risks of devices used in the business operation, such as mobile device management (MDM).*
2.8.6 Data Backup	
8.6 Sensitive data should be backed up using an appropriate method and frequency to ensure the availability of data consistent with the goal of restoring the IT system where the IT system and primary data were interrupted or damaged. Backup copies of data and the data recovery process shall be tested at least once a year.	1. A business operator should establish measures or processes for data backup, which are consistent with the recovery time objective (RTO) and the recovery point objective (RPO) which should at least contain the following details: (1) data to be backed up; (2) frequency or period of data backup; (3) data backup procedures and methods; (4) data recovery procedures and methods; and (5) storage site and methods for removable media. 2. The business operator should store the backup media, including a copy of relevant procedures outside the primary site or outside the main operating premises. These sites should have security measures that are equivalent to those of the primary site or the main operating premises. 3. The business operator should conduct a review of data backup and testing of backup data at least once a year to ensure the integrity, availability, and security of the backup data. 4. Where it is necessary to store data for a long period of time, the business operator should consider the method

Provisions in Appendix 3 Attached to the *Notification No. Sor. Thor. 38/2565*	Guidelines
	for reusing such data in the future in case of necessity. For example, when data were stored on certain media, the device and program used to read such media should also be stored.
2.8.7 IT System Logging	
8.7 IT system logs shall be produced and stored completely and adequately for use as evidence of electronic transactions. They may also be used for monitoring and reviewing accesses to and uses of data and the IT system as required by law.	1. A business operator should keep logs by using a secure method with sufficient details for use as proof in the inspection, where the person performing the task can be identified. The logs should be retained for a minimum of 90 days, or as required by applicable laws. The logs should at least contain the following items: (1) physical access logs recording accesses to the computer site and areas that are related to the critical IT system; (2) authentication logs and access logs of servers, application systems, network equipment and sensitive data, including any log-in attempts. (3) activity logs of important activities, which should at least include the following details: (a) changes of data structure; (b) changes and deletions of sensitive data; (c) changes of system configuration; (d) changes of user accounts and rights; (e) Internet use through the business operator's network system; and (f) network firewall logs;

Provisions in Appendix 3 Attached to the *Notification No. Sor. Thor. 38/2565*	Guidelines
	(4)[2] proof of electronic messaging of access persons, containing at least the details of user IDs, date and time of access, and information on messages throughout the conversations which should be retained as evidence for a minimum of six months; and (5) transaction logs with a minimum retention period of one year. In the case of the securities trading system, the details should include user accounts, securities symbols, broker numbers (4-digit), SET order IDs, account IDs, date and time of transactions (yyyy/mm/dd - hh:mm:ss:sss), source public and local IP addresses, destination IP addresses, full URLs, and terminal type (if any, such as iPad and iPhone). 2. The business operator should synchronize the clock of the servers, application systems, and network equipment with the network time protocol (NTP) server to ensure that the time of logging is accurate and in a real-time manner. The NTP server should receive signals from reliable sources (such as Stratum 1 from the National Institute of Metrology and the Hydrographic Department, Royal Thai Navy). If the business operator who is a member of the Stock Exchange of Thailand ("SET") should synchronize the clocks of all IT equipment and system related to securities trading and clearing to the reference time of the SET's trading system to ensure correct and effective inspection of inappropriate transactions. 3. The business operator should keep logs of personal data for the purpose of examining user activities and as

[2] Applicable only to access persons of the business operator undertaking securities business in brokerage, dealing or underwriting of any securities, which is not limited to debt securities or investment unit, derivatives agent, and management of mutual funds or private funds.
The definition of "access person" shall be in accordance with the Notification of Guidelines on Policies, Measures and Processes Concerning Acts That May Cause Conflicts of Interest with Clients.

Provisions in Appendix 3 Attached to the *Notification No. Sor. Thor. 38/2565*	Guidelines
	evidence in the case of inappropriate accesses, change, or disclosure of personal data. The logs should comply with applicable laws and regulations, such as the law on computer-related crime and the law on personal data protection. 4. The business operator should store logs of important equipment on a separate logging server or use an equivalent method which can prevent change, amendment, or destruction of the logs, with minimum security measures as follows: (1) stipulating duties and responsibilities of log access persons as necessary; (2) having a strict process for authentication and verification of log access rights; and (3) installing a server or equipment used to store logs in a safe and secure network zone.
2.8.8 Security Monitoring	
8.8 Security monitoring involves using a process or tool to prevent and detect IT incidents, malware, or cyber threats which may affect the security of critical IT systems.	1. A business operator should implement a process or tool to detect unusual events which may compromise the security of their critical IT systems in a timely manner, such as a process or tool for reviewing logs, so as to be aware of incidents or threats and take appropriate preventative or responsive actions. 2. The business operator should put in place a process or tool for receiving cyber threat intelligence to enable monitoring and analysis of potential cyber threats and preventing or handling thereof appropriately. 3. *[High-risk] The business operator should have a unit responsible for surveillance, monitoring, analyzing, coordinating and acting as a center for threat management, such as a security operations center (SOC).* 4. *[High-risk] The business operator should have a system in place to collect incident data from various data sources, such as network equipment, operating systems, and network security systems, to be used in a log correlation process and analysis of security incident information.* 5. *[High-risk] The business operator should put in place a process or tool for detecting the change of files or*

Provisions in Appendix 3 Attached to the *Notification No. Sor. Thor. 38/2565*	Guidelines
	configuration on the critical IT system or critical IT equipment, such as file integrity monitoring (FIM) / file integrity checking on the servers that are connected to the Internet, and detection of configuration changes of significant network equipment (such as firewalls). 6. *[High-risk] The business operator should provide a process or tool for monitoring and alerting on suspicious user behavior, such as unusual network use, large data volume transfers, accessing the application system during irregular hours, or accessing the system from a computer that has never been used before.*
2.8.9 Technical Vulnerability Assessment	
8.9 Technical vulnerability assessment of the IT systems shall be conducted in accordance with the risk level to identify vulnerabilities and rectify them to prevent potential cyber threats in a timely manner. The technical vulnerability assessment of the critical IT systems and all internet-facing IT systems shall be conducted at least once a year and upon every significant change to such systems, such as changes to the IT infrastructure or addition of critical functions.	1. A business operator should specify the scope and frequency of technical vulnerability assessment to include all application systems based on the level of risk. For critical IT systems and all internet-facing IT systems, technical vulnerability assessment should be conducted at least once a year and upon every significant change to such systems. 2. A business operator should assess the risk of identified vulnerabilities and specify an appropriate rectification period. 3. A business operator should report the results of the vulnerability assessments to the responsible person, follow up on rectification, and ensure that such vulnerabilities are rectified within the specified period. The progress of the operation should be reported to the assigned committee or high-level executive.
2.8.10 Penetration test	
8.10 Penetration test 8.10.1 A business operator shall conduct penetration testing as follows:	1. A business operator should conduct penetration testing on application systems and internet-facing network systems at least once a year and upon every significant change to such systems. For other systems, an assessment

Provisions in Appendix 3 Attached to the *Notification No. Sor. Thor. 38/2565*	Guidelines
(1) internet-facing application systems and network systems: (1.1) at least once a year; and (1.2) upon every significant change to such systems (2) systems other than those in (1): Assessment of risk from intrusions through the internal network shall be conducted to specify the scope of penetration testing and conduct penetration testing as appropriate.	of intrusion risk through the internal network should be conducted to specify the scope of the penetration test as appropriate. 2. A business operator should evaluate the risk of identified vulnerabilities and set an appropriate rectification period. 3. A business operator should report a summary of penetration test results to the relevant responsible persons, such as the unit that owns the system, the compliance unit, or the internal audit unit, including following up on the rectification of vulnerabilities to ensure that they are carried out within the specified period. The progress of the operation should be reported to the assigned committee or high-level executive. 4. A business operator should collect and analyze vulnerabilities detected to help establish security measures for future IT systems.
8.10.2 The aforementioned penetration testing shall be carried out by in-house experts or external experts independent of the system owner.	1. A business operator should specify that the penetration tester must be knowledgeable in and experienced with penetration testing and independent from the unit owning the system and independent from the development of such system. 2. *[High-risk] A business operator should specify that the penetration tester conducting penetration testing on critical IT systems must possess accreditations and certifications recognized in the industry, such as:* *(1) certifications from the Council for Registered Ethical Security Testers (CREST), such as CREST Registered Penetration Tester, CREST Certified Web Application Tester, and CREST Certified Infrastructure Tester;* *(2) certifications from Offensive Security, such as Offensive Security Certified Professional (OSCP), Offensive Security Wireless Professional (OSWP), Offensive Security Certified Expert (OSCE), Offensive Security Exploitation Expert (OSEE), and Offensive Security Web Expert (OSWE); and* *(3) certifications from Global Information Assurance Certification (GIAC), such as GIAC Certified Incident Handler*

Provisions in Appendix 3 Attached to the *Notification No. Sor. Thor. 38/2565*	Guidelines
	(GCIH), GIAC Mobile Device Security Analyst (GMOB), GIAC penetration tester (GPEN), GIAC Exploit Researcher and Advanced Penetration Tester (GXPN), GIAC Assessing and Auditing Wireless Networks (GAWN), and GIAC Web Application Penetration Tester (GWAPT). *The business operator may consider other certifications comparable to the foregoing certifications.*
8.10.3 In the event that any vulnerabilities are identified, a business operator shall take steps to rectify them and prevent potential cyber threats in a timely manner to eliminate any risk from such vulnerabilities.	[No specific guidelines have been prescribed.]
8.10.4 A business operator shall retain reports of operations under Clause 8.10 for a minimum of two years from the date of creation, in a way that such documents are readily available upon request for inspection by the SEC Office.	1. A business operator should prepare a report on penetration testing results, including important details, such as the scope of testing, test period, tester, penetration test methods and procedures, and identified vulnerabilities, as well as a plan to rectify such vulnerabilities based on the risk level. This report should be retained a minimum of two years from the date of creation and readily available upon request for inspection by the SEC Office.
8.10.5 A business operator shall submit the report on penetration testing results without delay upon notification by the SEC Office.	[No specific guidelines have been prescribed.]
2.8.11 Patch Management	
8.11 There shall be patch management by putting in place a process to control the installation of patches on systems and	1. A business operator should establish standards and regulations for patch management covering at least the following operations: (1) assessment of risk and necessity for patch installation;

Provisions in Appendix 3 Attached to the *Notification No. Sor. Thor. 38/2565*	Guidelines
equipment to reduce the risk of potential attacks.	(2) stipulation of a time frame for patch installation by taking into consideration the necessity and risk of attacks due to vulnerabilities; and (3) verification and testing of patches before their installation on the production systems to prevent undesirable impacts from installation of patches. If there is any restriction on patch testing, the business operator may consider other types of control instead. 2. The installation of patches on production systems should be carried out according to the established change management process to prevent risks and errors in the operation. 3. If the application system or equipment manufacturer has not officially announced the update of security patches to fix the newly identified vulnerabilities, the business operator should follow the instructions of the system developer, product owner, or security expert, or should put in place a substitute control measure to reduce the risk of being attacked through such vulnerabilities. 4. *[High-risk] The business operator should provide a patch monitoring tool that has not yet been installed on the business operator's critical operating system and database system.*
2.9 Communication System Security	
Part 9 Communication System Security A business operator shall have appropriate communication system security to ensure that the communication system and data transmitted through the communication system will be safe and secure and can prevent potential cyber intrusions or threats as well as being able to	1. A business operator should put in place a communication system security by undertaking at least the following acts: (1) designing communication networks with proper network segregation, by taking into account the level of importance of the application systems and the level of importance of data, including the necessity for connection from other application systems or outside the organization; (2) putting in place strict control of connection of critical application systems; (3) for the segregation of systems to ensure safety, the following acts should be undertaken:

Provisions in Appendix 3 Attached to the *Notification No. Sor. Thor. 38/2565*	Guidelines
provide continuous services.	(a) separating the private network from the public network; (b) segregating the network of the critical IT system from the network for operation by employees, the network for general use and the guest network; (c) at the point of segregation of networks that are critical and at risk, a network security tool with the ability to control and screen traffic transmitted through the networks should be installed to prevent and detect intrusion by viruses or malware; (4) controlling and allowing only authorized equipment to connect to internal networks; (5) activating connection ports only as necessary. In the case where inactivated ports must be used, a process for applying for approval from the authorized person should be prescribed and appropriate control should be implemented; (6) monitoring the availability of networks to ensure that they are in line with the established service level agreement (SLA); (7) providing a system or measure to prevent attacks through the public network that is suitable for the risk, such as using intrusion prevention system (IPS) security devices and DDoS protection; (8) *[High-risk] the business operator should install network security devices to screen traffic at the application level at the point of connection to public network, such as the use of web application firewall (WAF); and* (9) *[High-risk] ensuring that access to network equipment and security devices for configuration management is made through a network separate from the regular network to prevent unauthorized changes to network equipment and network security devices.* 2. A business operator should maintain the security of information transmitted through communication networks by undertaking at least the following acts:

Provisions in Appendix 3 Attached to the *Notification No. Sor. Thor. 38/2565*	Guidelines
	(1) establishing best practices for information transmitted through various types of electronic communication channels; (2) applying data encryption techniques in the transmission of confidential and sensitive information; and (3) putting in place measures to protect confidential or sensitive data transmitted in the form of attachment files and automatically forwarded email to external entities. 3. A business operator should put in place security measures for the use of the electronic messaging system by undertaking at least the following acts: (1) putting in place measures to prevent unauthorized changes, damage, or access to data in the electronic messaging system; (2) putting in place an appropriate user authentication process by requiring a stronger level of authentication if the electronic messaging system is used through a public network; (3) in the case of using the electronic messaging system provided by a third-party service provider, such as instant messaging, social networking, or file sharing, the business operator should ensure appropriate and adequate control thereof and consider strict compliance with applicable laws and regulations; (4) filtering emails at risk of cyber threats, such as email with .exe attachments; and (5) *[High-risk] The business operator should put in place a process or tool simulating virtual environment (secure container/virtual environment) to analyze the attack behavior from data and file attachments in user email, such as the use of sandbox tools and the advanced threat protection (ATP) system.*
2.10 IT Project Management and System Acquisition, Development, and Maintenance	
Part 10 IT Project Management and System Acquisition, Development, and Maintenance	

Provisions in Appendix 3 Attached to the *Notification No. Sor. Thor. 38/2565*	Guidelines
A business operator shall have IT project management and IT system acquisition, development and maintenance to ensure security throughout the entire life cycle of its IT systems as follows:	
2.10.1 IT Project Management	
10.1 IT Project Management Establishing a project management framework to ensure efficient management of significant IT project, ensuring they are delivered accurately and completely as planned and the specified goals are achieved.	1. A business operator should establish a project management framework in writing, including the following minimum details: (1) a clear project governance framework to ensure successful project execution according to the established plan, by assigning responsible persons with roles and responsibilities as necessary and as appropriate, such as: (a) a project steering committee, responsible for overseeing and monitoring project progress, providing advice, and making decision on operations in critical projects to ensure project execution as planned. The committee should consist of executives from related units and the project owner/project sponsor; (b) a project management office or team, responsible for establishing standard formats, processes, and tools for managing and monitoring project progress, including reporting the overview of the business operator's critical projects to its board of directors and relevant high-level executives for their acknowledgment to enable achievement of established goals; and (c) the project manager, responsible for managing projects in compliance with project management rules and procedures to ensure correct delivery and completion as planned; (2) guidelines on project management, including the following minimum details:

Provisions in Appendix 3 Attached to the *Notification No. Sor. Thor. 38/2565*	Guidelines
	(a) rules and procedures for project management, covering from pre-commencement of the project, project operation and control, to project closure and project review; (b) explicit factors and criteria for assessing or prioritizing projects, including scope of authority for project approval and overseeing projects based on the level of importance; and (c) explicit documents or deliverables for each phase, such as a project plan, progress report, and project closure report. 2. For project commencement, the business operator should undertake at least the following acts: (1) assess the necessity and expected benefits, including potential risks and impacts on systems and functions related to the projects; (2) prepare a detailed and adequate project plan for project management, which should at least cover the following matters: (a) project goals; (b) resources and technologies used; (c) roles and responsibilities of the project team members; (d) scope and duration of each stage of the project; (e) deliverables in each phase; and (f) requirements and conditions related to the projects (if any), such as requirements of the employer, obligations, and restrictions; (3) present the project plan to the business operator's board of directors, the assigned committee, or high-level executives for approval based on the established scope of approval. 3. For the operation and control of projects, the business operator should undertake at least the following acts:

Provisions in Appendix 3 Attached to the *Notification No. Sor. Thor. 38/2565*	Guidelines
	(1) continuously monitor and assess the operation of projects, which should cover the planned scope, duration and resources; (2) in the case of changes in the scope, duration, or resources or if projects are cancelled, present these changes or cancellations for approval to the authorized person; and (3) report project progress, problems, obstacles, and restrictions to the project steering committee or the assigned high-level executives on a regular basis. Projects which significantly affect the business operator's business should also be presented to the business operator's board of directors or the committee assigned by such board of directors. 4. For project closure, a business operator should undertake at least the following acts: (1) summarize benefits received from the projects in comparison to the established goals; and (2) collect any problems and obstacles encountered during project management and utilized them as lessons learned for the purpose of analyzing, improving, and developing more efficient processes or tools for future project management. 5. A business operator should review significant projects to ensure alignment with the project goals, policies, standards, rules and practices of the business operator, including compliance with relevant laws and regulations. 6. *[High-risk] The business operator should require that the reviewer of critical projects to be independent of the project operators, such as through the engagement of a project quality assurance unit.*
2.10.2 System Acquisition	
10.2 System Acquisition Criteria for acquisition of IT systems and service providers shall be established to ensure that the	1. A business operator should establish criteria for selecting IT systems and service providers to ensure that the systems acquired can meet the business requirements and information security requirements, which should take into consideration the following matters:

Provisions in Appendix 3 Attached to the *Notification No. Sor. Thor. 38/2565*	Guidelines
acquired systems meet the business requirements and IT security requirements. The criteria shall take into account the flexibility of changing service providers, changes in technology, and changes that are significantly related to business operations.	(1) general details, such as the technology used, software license, and system functions; (2) system security; (3) reliability of IT systems and service providers, such as financial position, reputation, and technical capabilities; (4) certification according to international standards or related IT standards that are generally recognized; (5) system support and maintenance; (6) proof of concept in the case of a critical IT system; and (7) measures to accommodate or manage risks in the case that a system developer or software service provider fails to comply with the agreement on system maintenance or operational support, such as a source code escrow agreement, to ensure that the business operator will have the right to access the source code of such systems or software.
2.10.3 System Development	
10.3 System Development Control measures in relation to IT system development including designing, developing, system testing, and deploying the system shall be established to ensure that the system is accurate, secure, reliable, ready for use, and adequately flexible to accommodate usage and aligned with the business plan, by undertaking at least the following acts:	[No specific guidelines have been prescribed.]

Provisions in Appendix 3 Attached to the *Notification No. Sor. Thor. 38/2565*	Guidelines
(1) establishing detailed requirements of the system and technical specifications of the developed system as follows: (1.1) security; (1.2) availability; and (1.3) capacity.	<u>System Design</u> 1. A business operator should require the relevant business units to contribute to the establishment of system requirements details. 2. The business operator should prepare a document specifying details of functional requirements and non-functional requirements of the system and technical specifications of the system, covering the following issues: (1) security according to the policy or standards set by the business operator, such as access control and data encryption; (2) availability, such as designing the system to have high availability or redundancy, including a backup system (DR strategy), to enable the system to provide continuous service and reduce the risk of a single point of failure; and (3) capacity. The forgoing document should be reviewed for completeness and accuracy and approved by the related persons before system development begins.
(2) segregating roles and responsibilities of persons involved in system development to ensure that the system will be reviewed before deploying into production;	<u>System Development</u> 1. A business operator should segregate duties and responsibilities of persons involved in system development to enable review before system deployment, such as segregating system developers from those who deploy the system.
(3) segregating the environments of the application systems used for development and testing from production;	1. A business operator should separate development and testing environments from production environments to control the testing and to reduce any potential impact that may affect the production system. 2. A business operator should implement security measures for non-production systems that are sufficient for the risk of unauthorized access to the system and data and the leakage of data used in testing.

Provisions in Appendix 3 Attached to the *Notification No. Sor. Thor. 38/2565*	Guidelines
	3. A business operator should implement controls to prevent the installation of development tools and compilers on production systems to prevent the risk of unauthorized changes or installations of programs.
(4) putting in place a process or tool to ensure secure source code development;	1. A business operator should establish standards and procedures for secure coding that align with international standards, and ensure that developers comply with these standards and procedures. 2. A business operator should have processes or tools for source code version control. 3. A business operator should conduct source code reviews by using either automated tools (automated reviews) or manual reviews by a person not involved in the development, upon development or changes of critical IT systems with security risks, in order to identify and correct security defects before deployment. 4. *[High-risk] A business operator should conduct manual source code reviews which should be carried out by an expert who is independent of the program developer upon development or changes of critical IT systems with security risk.*

Provisions in Appendix 3 Attached to the *Notification No. Sor. Thor. 38/2565*	Guidelines
(5) conducting testing on the IT system that has been developed or changed to ensure that such system will be able to accurately and comprehensively process data and meet the needs of users;	<u>System Testing</u> 1. A business operator should arrange system testing before going live to ensure that such systems can operate correctly, securely, efficiently, and as required by users. Testing should at least cover the following matters: (1) unit test; (2) system and integration test; (3) user acceptance test; and (4) security test, vulnerability assessment, and penetration test as necessary for any new system connected to critical IT systems to enable the detection of vulnerabilities and correction thereof appropriately before going live. 2. A business operator should specify end-to-end test scenarios or test cases and have a process to review the test scenarios or test cases to ensure that they are adequately comprehensive and meet the business requirement. 3. A business operator should test the system in an environment that is similar to production to reduce potential risks from the changes in production. 4. A business operator should manage defects of the system found in testing by considering ways to improve or reduce the risks and impacts of such defects. 5. The business operator should apply for approval of the test results from the relevant unit prior to system deployment.
(6) having measures to ensure the integrity of data conversion;	1. The measures ensuring the integrity of data conversion should cover data migration cases, such as storage migration, cloud migration, or application migration.

Provisions in Appendix 3 Attached to the *Notification No. Sor. Thor. 38/2565*	Guidelines
(7) having measures to maintain the security and privacy of sensitive data used in testing;	1. If sensitive data from the production system are used in system testing, a business operator should implement security and privacy measures on such data, such as data masking, to prevent the risk of data leakage.
(8) conducting a performance test of systems related to electronic channels services or electronic transactions upon significant development or change of the systems, to ensure that such systems able to support the number of concurrent users and transactions in line with business requirements;	[No specific guidelines have been prescribed.]
(9) in the case that a third party is assigned to develop or change IT systems, a business operator shall monitor and ensure that their operations comply with the agreement; and	[No specific guidelines have been prescribed.]
(10) having a process for application of approval from management or the committee assigned by the business operator before system deployment.	<u>System Deployment</u> 1. A business operator should deploy the system using the established change management procedure. 2. A business operator should prepare system deployment by archiving the version before the change in such a way that it is readily available for restoration. 3. A business operator should establish a cutover plan or go-live technique suitable for the level of risk, such as direct changeover, parallel changeover, or phased changeover.
2.10.4 System Change	

Provisions in Appendix 3 Attached to the *Notification No. Sor. Thor. 38/2565*	Guidelines
10.4 System Change	1. A business operator should implement changes to IT systems in compliance with the guidelines on change management and system development.
(1) Conducting impact assessments and prioritization of change;	[No specific guidelines have been prescribed.]
(2) Establishing a process for requesting change approval, which must be granted in writing by the system owner unit to ensure the necessity for the change has been appropriately considered;	[No specific guidelines have been prescribed.]
(3) Conducting tests before configuring or deploying changes to production to reduce potential risks or impacts;	[No specific guidelines have been prescribed.]
(4) Having a process for approving the release of changes to production from management or the committee assigned by the business operator;	[No specific guidelines have been prescribed.]
(5) Implementing a procedure or tool that controls source code version changes and supports fallback; and	[No specific guidelines have been prescribed.]

Provisions in Appendix 3 Attached to the *Notification No. Sor. Thor. 38/2565*	Guidelines
(6) Updating supporting documents of application systems that have been changed.	1. A business operator should always update operating procedures, backup systems, and business continuity plans in response to any IT system changes. In addition, such changes should be communicated to relevant persons for acknowledgement to enable proper performance of work.
2.11 IT Incident Management	
Part 11 IT Incident Management A business operator shall appropriately and timely manage IT incidents as follows:	
11.1 provide a point of contact for reporting of IT incidents by personnel, clients, and relevant parties;	1. A business operator should assign the responsible person or unit to serve as a point of contact for reporting of incidents. The point of contact should record data, perform initial rectification, or forward incidents to the relevant IT unit.
11.2 establish a plan or procedure for management of IT incidents;	1. A business operator should establish an incident management plan or incident response plan, based on the significance of incidents, to facilitate the handling of and response to incidents in a prompt and timely manner. The plan should include at least the following details: (1) verification of reported incidents; (2) classification and assessment of the urgency of incidents to ensure a timely response; (3) incident response process, including incident analysis, containment, evidence gathering, resolution research, and eradication and recovery as well as a channel for coordination with internal and external experts; (4) guidelines on reporting of incidents (incident escalation) and progress reporting to the business operator's top management and the board of directors, based on the level of severity of incidents; (5) notification or communication to clients, including the designation of a responsible person for communication and the identification of communication channels to inform the clients of the impacts and

<table>
<tr><th>Provisions in Appendix 3
Attached to the Notification No. Sor. Thor. 38/2565</th><th>Guidelines</th></tr>
<tr><td></td><td>progress of incident resolution. This should also include the provision of advice on alternative service options during the period in which the services are impacted by the incidents, to ensure that clients have options for managing their transactions; and
(6) in the case of a cybersecurity incident with significant impacts on client assets and data, conducting a digital forensic investigation with the assistance of experts to identify the causes or vulnerabilities of the system and safely patch any vulnerabilities.</td></tr>
<tr><td>11.3 reporting IT incidents, personal data breaches, and IT system security incidents that causing damage to client’s assets to the responsible person and the SEC Office without delay upon discovery of such incidents;</td><td>1. A business operator should report incidents of violation of laws, rules, and regulations applicable to the business operator to the relevant agency without delay and within the time frame specified by law. Such incidents include, but are not limited to, incidents with large-scale impacts on clients which should be reported to the SEC Office within three hours, and leakage of client’s personal data which shall be reported to the Office of Personal Data Protection Committee within 72 hours.
2. The business operator should report to the SEC Office any IT incidents which may have large-scale impacts on the operations, business, reputation, financial status, and operating performance of the business operator or clients. These incidents include, but are not limited to:
(1) personal data breach caused by IT incidents;
(2) loss or damage of clients’ assets;
(3) unauthorized intrusion, access, or use of the system (system compromised);
(4) incidents that harm the business operator’s reputation, such as the company’s website defacement; and
(5) system disruption during the business operator’s business hours as follows:
<table>
<tr><th>Application System</th><th>Duration of Disruption Before Reporting to the SEC Office</th></tr>
</table>
</td></tr>
</table>

Provisions in Appendix 3 Attached to the *Notification No. Sor. Thor. 38/2565*	Guidelines

Order matching system	All cases of disruption
Order management system or trading system	15 minutes
Other systems, such as the main website and the asset deposit and withdrawal system	60 minutes

These disruptions do not include system maintenance for which clients have been notified in advance.

3. A business operator should report an incident to the SEC Office within the following time frames:

3.1 **If an incident was discovered on a business day of the SEC Office during 8.30 a.m. – 4.30 p.m.:**

(1) report the incident promptly within three hours upon the discovery of the incident. The content should contain the date, time, type of incident, incident details, and expected impacts. The reporting may be made verbally or through the electronic channel as specified by the SEC Office, as deemed appropriate.

(2) report progress upon any changes in the circumstance or as requested by the SEC Office, until the IT system returns to normal service. The content should contain the date, time, type of incident, incident details, realized impact, and resolution progress. The reporting should be made through the electronic channel specified by the SEC Office; and

(3) report the incident upon its conclusion or completion of incident resolution. The content should contain the date, time, type of incident, incident details, realized impact, resolution, outcome of resolution, duration of resolution, cause of the incident, and future incident preventive measures. The reporting should be made through the electronic channel specified by the SEC Office.

For example: (in the case of a securities company) an incident was discovered at 8.30 a.m. on Friday, September 1st:

Provisions in Appendix 3 Attached to the *Notification No. Sor. Thor. 38/2565*	Guidelines
	- report the incident according to (1) within 11.30 a.m. of Friday, September 1st; - report progress on the incident according to (2)upon changes in the circumstance or as requested by the SEC Office until the IT system returns to normal service; and - report the incident according to (3) upon the incident's conclusion or completion of incident resolution. 3.2 **If an incident is discovered outside the business hours specified in 3.1:** (1) report the incident without delay within 10.00 a.m. of the following business day,[3] by including the date, time, type of incident, incident details, and expected impacts. The reporting may be made verbally or through the electronic channel as specified by the SEC Office, as deemed appropriate. (2) report progress upon any change in the circumstance or as requested by the SEC Office until the IT system returns to normal service. The content should contain the date, time, type of incident, incident details, the realized impact, and resolution progress. The reporting should be made through the electronic channel specified by the SEC Office; and (3) report the incident upon its conclusion or completion of incident resolution. The content should contain the date, time, type of incident, incident details, the realized impact, resolution, outcome of resolution, duration of resolution, cause of the incident, and future incident preventive measures. The reporting should be made through the electronic channel specified by the SEC Office. <u>For example:</u> (in the case of a securities company) an incident was discovered at 03.30 a.m. on Friday, September 1st:

[3] "Business day" shall mean a business day of the SEC Office.

Provisions in Appendix 3 Attached to the *Notification No. Sor. Thor. 38/2565*	Guidelines
	- report the incident according to (1) within 10.00 a.m. of Friday, September 1st; - report the progress on the incident according to (2) upon changes in the circumstance or as requested by the SEC Office until the IT system returns to normal service; and - report the incident according to (3) upon the incident's conclusion or completion of incident resolution. 4. In the case of a critical information infrastructure organization or CII organization[4], an incident shall be reported to the SEC Office and relevant regulators within the time frame as prescribed by the National Cybersecurity Committee.
11.4 conducting a root cause analysis of any IT incident to establish guidelines on resolution and prevention of future recurrence of such incident;	1. A business operator should conduct a root cause analysis of any IT incident and use the lessons learned from such incident to prevent future recurrences or improve the process for responding to incidents more efficiently.
11.5 recording data related to IT incident management and storing such data for a minimum of two years from the date of such incident, in a way that such data are readily available upon request for inspection by the SEC Office; and	1. A business operator should record and store data related to IT incidents in a standard format. This data should include, but not be limited to, the date and time of the incidents, the incidents details, impacts, resolution methods, date and time of the incidents' resolution, causes of the incidents, and future incident preventive measures. Such data should be retained for a minimum of two years from the date of such incidents, in a way that such data are readily available upon request for inspection by the SEC Office.

[4] "Critical information infrastructure organization" shall mean a government agency or private organization with tasks or services providing critical information infrastructure. The characteristics of an organization with tasks or services providing critical information infrastructure shall be as prescribed by the National Cybersecurity Committee in its notification.

Provisions in Appendix 3 Attached to the *Notification No. Sor. Thor. 38/2565*	Guidelines
1 1 . 6 testing and reviewing IT incident management procedures or plans at least once a year. The testing shall cover the management of cyber security threats (cyber security drills). The results of these testing and review shall be reported to the business operator's board of directors or the committee assigned by such board of director.	1. A business operator should conduct testing and review of IT incident management procedures or plans at least once a year to be able to resolve incidents and return to normal state promptly and limit the damage to its business, by undertaking the following acts: (1) providing risk scenarios of potential cyber threats that align with the nature, scope and complexity of business operations and cyber threat trends that may impact the business operator. Such scenarios should be those that, if they occur, would significantly affect the IT system; (2) storing and updating all documents related to the testing, including: (a) risk scenarios, test scenario, date, time and test location, roles and responsibilities of persons involved in the test; and (b) summarizing the test results and results of incident management procedures review; (3) reporting the test and review results to the business operator's board of directors or the committee assigned by such board of directors; and *(4) [High-risk] reporting the test and review results to the business operator's board of directors.*
2.12 IT Contingency Plan	
Part 12 IT Contingency Plan A business operator shall establish an IT contingency plan to address IT incidents that impede normal service or continuous business operations. The business operator shall have the capability to restore the system to its normal state within a reasonable time frame, as follows:	

Provisions in Appendix 3 Attached to the *Notification No. Sor. Thor. 38/2565*	Guidelines
12.1 appointing a task force or a unit responsible for preparation of an IT contingency plan;	1. A business operator should appoint, in writing, a task force or a unit responsible for preparation of an IT contingency plan with participation by executives and personnel from relevant units, such as the IT unit, business unit, and corporate communication unit.
12.2 establishing a process for preparation of an IT contingency plan as follows: 12.2.1 conducting a risk assessment to identify risk scenarios that may disrupt the IT processes and systems, thereby causing the business operator to be unable to provide normal services or operate business continuously;	1. A business operator should conduct a risk analysis to identify risk scenarios that may disrupt IT processes and systems, thereby causing the business operator to be unable to provide normal services or operate business continuously, as follows: (1) specify risk scenarios that may disrupt the IT processes and systems, both from within and outside the organization; (2) conduct risk analysis by considering impacts and likelihood, including existing controls; and (3) provide a process and resources necessary to control the risks, ensuring that they are at the acceptable level.
12.2.2 conducting business impact analysis due to the risk scenarios under 12.2.1 to prescribe the appropriate recovery time objective (RTO), recovery point objective (RPO), and maximum tolerable downtime (MTD); and	1. A business operator should conduct a business impact analysis to prioritize the importance of the IT system that affects business operations, with the following operational guidelines: (1) specify business processes and the IT systems on which the businesses rely; (2) analyze the impacts from the disruption of the IT systems to prescribe the RTO, RPO, and MTD periods, provided that: (a) RTO for the IT systems that support the critical business processes of a critical information infrastructure organization or CII organization should not be longer than two hours; and (b) RTO for the IT systems that support the critical business processes of other business operators should not be longer than four hours. If the business operator is unable to stipulate the RTO of the IT

Provisions in Appendix 3 Attached to the *Notification No. Sor. Thor. 38/2565*	Guidelines
	systems as required above, the business operator may use a manual service method instead, provided that such method must not significantly affect the efficiency of the services; (3) specify the IT systems and resources necessary for the critical business processes (hardware, software, data, and other resources), including minimum specifications of such IT systems and resources; and (4) IT systems prioritization to ensure that the IT systems which support highly critical business processes are recovered first.
12.2.3 preparing a written IT contingency plan approved by the business operator's board of directors or the committee assigned by such board of directors;	1. A business operator should establish an IT contingency plan approved by the business operator's board of directors or the committee assigned by such board of directors. The plan should contain clear and easy-to-follow processes or procedures to enable prompt implementation and should at least include: (1) roles and responsibilities of high-level executives and persons involved in the execution of the plan; (2) description of the IT systems, such as system architecture and network diagrams; (3) conditions and procedures for activating the IT contingency plan, procedures for responding to emergency incidents, and the plan for communicating to relevant parties; (4) procedures for system and data recovery with clear and sufficient details that can be properly followed by the operators, and within the established time frame, which may be presented in the form of a checklist; (5) procedures for verifying the integrity of the recovered IT system and data before resuming normal business operations; (6) procedures for announcing the cancellation of the IT contingency plan; and (7) storing the IT contingency plan in a safe place and making it available for use at the primary operation site and the backup site. 2. A business operator should provide a list of personnel and their contact channels to be used for communication

Provisions in Appendix 3 Attached to the *Notification No. Sor. Thor. 38/2565*	Guidelines
	in the event of a crisis or urgent situation. 3. *[High-risk] The IT contingency plan should be approved by the business operator's board of directors.*
12.3 providing a backup IT system and necessary resources to enable system recovery according to the established recovery time objective;	1. A business operator should provide a backup IT system and necessary resources to enable system recovery according to the established recovery time objective. If the business operator has a backup data center, it should specify clear description of the data center, such as available resources, location, and the map.
12.4 communicating the IT contingency plan to relevant personnel to ensure they understand and are able to comply with the IT contingency plan appropriately;	1. A business operator should communicate the IT contingency plan to all employees involved in actions under the plan so that they understand and can comply properly with it.
12.5 reviewing and testing the IT contingency plan at least once a year and upon occurrence of any event that should undergo such review and test. The results of these testing and review shall be reported to the business operator's board of directors or the committee assigned by such board of directors;	1. A business operator should review and test the IT contingency plan at least once a year and upon occurrence of any event that necessitates such review and testing, such as changes in business strategies, overall risk management policy, service or business environment, resources, or the IT system structure. 2. A business operator should specify test scenarios used in the annual test. The test scenario should be an event that may occur and disrupt critical business processes, such as disruption of the IT system supporting critical business processes, disruption of critical third-party service providers (including cloud service providers), and cyber-attacks. 3. A business operator should report the results of the IT contingency plan test to the business operator's board of directors or the committee assigned by such board of directors, with details at least covering the test objectives, scope of the test, scenarios, test results, errors, and problems or obstacles detected, as well as guidelines on improvement and rectification of the plan. 4. *[High-risk] A business operator should report the results of IT contingency plan test to the business operator's*

Provisions in Appendix 3 Attached to the *Notification No. Sor. Thor. 38/2565*	Guidelines
	board of directors, with details at least covering the test objectives, scope of the test, scenarios, test results, errors, and problems or obstacles detected, as well as guidelines on improvement and rectification of the plan. 5. *[High-risk] The business operator should test the IT contingency plan which should include the change of the business process or migration of data processing to the backup computer site/backup IT system.*
12.6 stipulating processes to handle incidents of IT resources overusing or exceeding the capacity of the specified indicators, such as limiting services through certain channels or disconnecting from a service provider or third party that affects the IT system; and	[No specific guidelines have been prescribed.]
12.7 providing the following contact information to enable efficient coordination of reporting IT incidents or requesting assistance from relevant external agencies, and such information shall be regularly updated: 12.7.1 a list of regulators and third parties that provide services or are connected to the IT systems of the business operator; and 12.7.2 contact channels and a list of relevant persons of the regulators or third parties under Clause 12.7.1.	[No specific guidelines have been prescribed.]

Chapter 3 Information Technology Audit

A business operator shall undertake the acts as prescribed in this Appendix.

Provisions in Appendix 4 attached to *Notification No. Sor Thor. 38/2565*	**Guidelines**
1. <u>Provision of an auditor</u> An auditor under 1 shall possess the following characteristics: 1.1 being independent of IT personnel at the following levels: 1.1.1 First Line of Defense: Operations; and 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; or 1.2.5 other certificates as additionally stipulated on the website of the SEC Office.	[No specific guidelines have been prescribed.]
2. <u>Audit Planning and Audit Scope Defining</u> 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*.	[No specific guidelines have been prescribed.]
3. <u>IT Audit under the Established Plan and Scope</u> 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	1. In the case of a small-scale business operator and a low-risk business operator (1) During a year in which a comprehensive audit of all

Provisions in Appendix 4 attached to *Notification No. Sor Thor. 38/2565*	Guidelines
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. 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 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 retained in a way that they will be readily available for inspection upon request by the SEC Office.	applicable rules (full-scope audit) is not conducted, the business operator may stipulate a scope of IT audit upon a risk-based basis. (2) During a year in which a comprehensive audit of all applicable rules (full-scope audit) is conducted, the business operator should arrange for a full-scope audit that covers every topic of the guidelines within that year.
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. The implementation progress of such plan shall be monitored.	[No specific guidelines have been prescribed.]
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.	Examples of how to determine the period for submitting the report on audit results to the SEC Office: (1) If the audit commences on August 15th and ends on September 30th, and the report and the corrective action plan are presented to the business operator's board of directors or the business operator's audit committee on October 15th, the business operator shall comply with the following time frames:

Provisions in Appendix 4 attached to *Notification No. Sor Thor. 38/2565*	Guidelines
5.2 [5]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:* 5.2.1 30 days from the date of presenting the audit report and corrective action plan to the business operator's board of directors or the business operator's audit committee; 5.2.2 90 days from the 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	● within 30 days from submission thereof to the business operator's board of directors or the business operator's audit committee, i.e., by November 14th; ● within 90 days from the end of the audit, i.e., by December 29th; or ● within three months from the end of the year in which the audit commences, i.e., by March 31st. The earliest due date is November 14th, therefore, the business operator shall submit the report to the SEC Office by November 14th. (2) If the audit commences on December 15th and ends on January 20th, and the report and corrective action plan are presented to the business operator's board of directors or the business operator's audit committee on March 5th, the business operator shall comply with the following time frames: ● within 30 days from submission thereof to the business operator's board of directors or the business operator's audit committee, i.e.,

[5] A business operator that is a commercial bank under the law on financial institution business, a life insurance company under the law on life insurance or a financial institute established under other laws, which has only been granted a license to undertake the following types of securities business, while does not undertaking 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.

Provisions in Appendix 4 attached to *Notification No. Sor Thor. 38/2565*	Guidelines
request by the SEC Office.	by April 4th; ● within 90 days from the end of the audit, i.e., by April 20th; or ● within three months from the end of the year in which the audit commences, i.e., by March 31st. The earliest due date is March 31st, therefore, the business operator shall submit the report to the SEC Office by March 31st.