Content

Title：	Directions for Operations Outsourcing by Securities Investment Trust Enterprises and Securities Investment Consulting Enterprises Ch
Date：	2023.08.31
Legislative：	1. Full text of 17 points adopted and issued per 31 August 2023 Order No. Financial-Supervisory-Securities-SITC-1120383717 of the Securities and Futures Commission; for immediate implementation Point 1 These Directions are adopted pursuant to Article 8, paragraph 1, subparagraph 18 of the Regulations Governing the Establishment of Internal Control Systems by Service Enterprises in Securities and Futures Markets and Article 8, paragraph 2 of the Standards Governing the Establishment of Securities Investment Consulting Enterprises. Point 2 A securities investment trust enterprise or securities investment consulting enterprise (hereinafter, "SITE/SICE") that will outsource operations to any third party (hereinafter, "outsourcing") shall enter a written agreement and comply with these Directions. However, if the outsourcing involves foreign exchange business, it shall additionally comply with the relevant rules and regulations set forth by the Central Bank. Point 3 The outsourcing by a SITE/SICE of operations involving business items it is permitted to engage in under the Securities Investment Trust and Consulting Act or other applicable laws and regulations or operations related to beneficiary or customer data shall be limited to the following scope:
Content：	1. Data processing: Including information system data entry, processing, output, and storage; development, monitoring, control, and maintenance of information systems; and logistical support for data processing in connection with conducting business. 2. Safekeeping of documents such as forms, statements, and certificates. 3. Securities investment trust fund overseas investment business, foreign exchange conversion business, exchange rate hedging management business. 4. Securities investment trust fund back-office account processing operations, including fund asset valuation, asset value calculation, accounting, etc. 5. Discretionary investment account back-office account processing operations, including asset valuation, asset value calculation, accounting, etc. 6. With respect to overseas investment of a securities investment trust fund or discretionary investment assets, engaging another member of the enterprise's business group or an overseas investment consulting company to provide centralized market trading services. 7. With respect to securities investment trust funds and discretionary investment assets, trading instruction operations for the creation and redemption of fund beneficial certificates. 8. With respect to overseas stocks held by securities investment trust funds, engaging another member of the enterprise's business group to exercise voting rights of the stocks, engaging a professional institution to provide analysis of motions to be voted on at shareholder meeting and services to assist with voting. 9. Matters that a SITE is legally permitted to outsource with respect to the handling of beneficial certificate transfer/registration services. 10. Other operations permitted for outsourcing pursuant to laws and regulations or approval by the competent authority.

A SITE/SICE shall file accurate reports on information including the items, content, and scope of its outsourced operations in the manner prescribed by the competent authority.

Point 4

A SITE/SICE shall conduct outsourcing operations in accordance with its internal outsourcing rules approved by its board of directors under the premises that outsourcing will not affect the sound operation of the SITE/SICE, the interests of beneficiaries or customers, or regulatory compliance.

The internal outsourcing rules referred to in the preceding paragraph shall specify the following contents:

1. Outsourcing policies and principles, including evaluation of outsourcing decisions, risk management mechanisms, approval hierarchy, and governance structure.
2. Division of authority and responsibility of the unit-in-charge and relevant units regarding the control of outsourced operations.
3. Scope of operations that may be outsourced and outsourcing procedures.
4. Internal operations and procedures for the protection of beneficiary or customer interests.
5. Risk management principles and operating procedures.
6. Internal control principles and operating procedures.
7. Other outsourcing operations and procedures.

A SITE/SICE is ultimately responsible for its outsourcing. It shall evaluate the risk level and materiality of outsourced operations and the impact of outsourcing on business operations and beneficiary or customer interests, adopt appropriate management measures under the risk-based approach, and comply with the following provisions:

1. The board of directors shall be aware of the outsourcing risks and regularly oversee the execution status of outsourced operations.
2. A SITE/SICE shall ensure that the unit-in-charge and relevant units have adequate resources, expertise, and authority over the control of outsourced operations.
3. A SITE/SICE shall identify, evaluate, and manage outsourcing of operations deemed material, and formulate relevant policies and procedures. It shall formulate enhanced controls and emergency response measures for outsourcing arrangements that may materially impact the normal operations of the SITE/SICE or beneficiary or customer interests.
4. A SITE/SICE shall have appropriate due diligence and periodic review procedures in place to ensure that service providers possess the expertise and resources for the execution of outsourced operations, are financially sound, have internal control and information security management mechanisms, and meet regulatory requirements.
5. A SITE/SICE shall ensure that the SITE/SICE itself and the competent authority, or persons designated thereby, can have access to relevant data or reports of service providers and conduct financial examinations or audits with respect to the outsourced operations, or order service providers to provide relevant data or reports within a prescribed time period.

The term "materiality" in these Directions means any of the following conditions:

1. The outsourced operation cannot be performed or there are concerns regarding information security, and such issues will materially impact business operations of the SITE/SICE.
2. The outsourced operation is involved in a beneficiary or customer data security incident, or a security incident involving investment portfolio details and transaction data of assets under management, that has a material impact on the interests of the SITE/SICE, beneficiaries, or customers.
3. The outsourced operation has otherwise had a material impact on the interests of the SITE/SICE, beneficiaries, or customers.

Point 5

When conducting outsourcing of operations in accordance with Point 3, paragraph 1, subparagraph 3 or 4 herein, a SITE/SICE shall, as provided in the Securities Investment Trust and Consulting Act and other applicable laws and regulations, apply to the competent authority for approval or file with it for recordation.

When conducting outsourcing of other operations approved by the competent authority in accordance with Point 3, paragraph 1, subparagraph 10 herein, a SITE/SICE shall apply to the competent authority for approval, submitting the following documents:
1. Internal outsourcing rules adopted in accordance with paragraph 2 of the preceding point.
2. Meeting minutes containing a resolution of the board of directors.
3. Necessity and legal compliance analysis of the outsourcing of business operations, evaluation of risk level and materiality of the outsourced operations and impact of the outsourcing on business and customer interests, due diligence check of service providers, and outsourcing risk management measures.
4. Operating process.
5. Other matters designated by the competent authority.
After an operation has been designated by the competent authority as eligible for outsourcing according to the preceding paragraph, other SITEs/SICEs may proceed directly to conduct that outsourcing operation in accordance with their internal outsourcing rules.
Point 6
The unit-in-charge specified in Point 4, paragraph 2, subparagraph 2 herein shall establish mechanisms for monitoring and supervising service providers, and shall carry out the following tasks:
1. Managing outsourced operations in accordance with the internal outsourcing rules set forth in accordance with Point 4 herein.
2. Supervising the outsourced operations in connection with the protection of beneficiary or customer interests, risk management and internal controls, conducting periodic evaluations and reviews, and submitting the findings to the board of directors.
3. Drafting and executing measures for selecting service providers, with contents including but not limited to the following:
A. Procedures for the evaluation and selection of service providers.
B. Standards for the appointment of service providers, which shall include ensuring that a service provider possesses the professional capabilities to handle the operation to be outsourced, and additionally ensuring that the outsourced operation is a business item that a service provider is legally allowed to operate.
C. Standards for evaluating the internal control operations and risk management of service providers.
D. Other conditions set forth by the competent authority.
Point 7
The internal operations and procedures for protection of beneficiary or customer interests included in the internal outsourcing rules of a SITE/SICE as provided in Point 4, paragraph 2, subparagraph 4 herein shall include the following contents:
1. If operations involve beneficiary or customer data, the agreement executed between the SITE/SICE and the beneficiary or customer shall include a provision that requires that the SITE/SICE inform the beneficiary or customer of the outsourcing. If the agreement does not include such a provision, the SITE/SICE shall notify its beneficiaries or customers of the outsourcing activity and the provisions of the Personal Data Protection Act shall apply.
2. Conditions and scope of beneficiary or customer data to be provided and procedural method for transferring such information.
3. Methods for supervising and mechanisms for managing the use, processing, and control of the aforesaid beneficiary or customer data by the service provider.
4. Procedures and time limits for handling beneficiary or customer disputes in connection of the outsourcing activity. The SITE/SICE shall set up a coordination unit that handles beneficiary or customer complaints.
5. Other necessary measures for the protection of beneficiary or customer interests.
A SITE/SICE shall be held equally liable to its beneficiary or customer as provided by law if an intentional act or omission or negligence of its outsourcing service provider or an employee thereof results in damage to beneficiary or customer interests.
Point 8

The risk management principles and operating procedures set forth in the internal outsourcing rules of a SITE/SICE as provided in Point 4, paragraph 2, subparagraph 5 herein shall include the following content:
1. Establishing a risk and benefit analysis system for outsourcing activity.
2. Establishing procedures or management measures sufficient to identify, measure, monitor, and control risks associated with outsourcing:
A. Evaluating the risk level and materiality of outsourced operations and their degree of impact on business operations.
B. Ensuring that the SITE/SICE and the service provider possess adequate expertise and resources.
C. Considering relevant risk factors, evaluating the risk level of outsourced operations, and taking appropriate measures to mitigate risk.
D. Evaluating risk levels periodically and ensuring updating of risk levels.
E. Conducting regular or unscheduled testing or drills based on different risk scenarios for material outsourcing.
3. Establishing an emergency response plan and transfer mechanisms for the termination of an outsourcing arrangement.
4. Other matters set forth by the competent authority.
Point 9
The internal control principles and operating procedures set forth in the internal outsourcing rules of a SITE/SICE as provided in Point 4, paragraph 2, subparagraph 6 herein shall include the following contents:
1. Drawing up and implementing the operating procedures for supervising and managing the scope of outsourcing.
2. Incorporating the operating procedures in the preceding subparagraph into the overall internal control system of the SITE/SICE for implementation.
3. Supervising the status of establishment and implementation of internal control and internal audit systems by the service provider.
4. Other matters set forth by the competent authority.
Point 10
A SITE/SICE's outsourcing agreement shall specify the following contents:
1. The scope and period of outsourcing and the authorities and responsibilities of the service provider.
2. A provision requiring the service provider to comply with Point 15 herein.
3. The SITE/SICE may instruct the service provider at any time on the outsourced operations and the service provider may not refuse.
4. Beneficiary or customer dispute resolution mechanisms, including the timetable and procedure for handling disputes, and remedial measures.
5. Protection of beneficiary or customer rights and interests, including data confidentiality and security measures.
6. The service provider is required to implement protection of beneficiary or customer interests, risk management, and internal control systems in accordance with the standard operating procedures established under the supervision or instructions of the SITE/SICE.
7. Material events that lead to the termination of an outsourcing agreement with the service provider, including a provision on termination or revocation of the agreement if so instructed by the competent authority.
8. The service provider agrees to allow the competent authority and the Central Bank to access relevant data or reports and conduct financial examination or auditing with respect to the outsourced items, or provide relevant data or reports within a prescribed time period pursuant to an order thereby.
9. The service provider shall not use the name of the outsourcing SITE/SICE in the course of handling the outsourced items, nor shall the service provider use untruthful advertising or collect fees from beneficiaries or customers.
10. The service provider is required to inform the SITE/SICE if the outsourced operation involves any material irregularities or deficiencies.
11. The law applicable to the contract and the court of venue and jurisdiction for litigation.
12. Other matters of agreement.
Subparagraphs 4 to 6 of the preceding paragraph do not apply if the

outsourced operations do not involve beneficiaries' or customers' rights and interests or their personal data.
If any existing outsourcing agreement does not conform to the provisions of these Directions, the SITE/SICE may continue its outsourcing activity under the existing agreement until it expires. However, if such agreement does not have an expiration date, the nonconformities shall be remedied within one year from the date these Directions are issued and enforced, or else the agreement will expire automatically.
Point 11
A SITE/SICE that plans to outsource operations to overseas service providers shall comply with the following provisions:
1. It shall fully understand and grasp the service provider's use, processing, and control of beneficiary or customer data or investment portfolio details and transaction data of assets under management.
2. Any beneficiary or customer data or investment portfolio details and transaction data of assets under management furnished to the service shall be limited solely to necessary data that is directly related to the outsourced operations.
3. Require the service provider to observe the following particulars:
A. The SITE/SICE's beneficiary or customer data or investment portfolio details and transaction data of assets under management shall be used and processed only by the authorized persons of the service provider within the scope of the outsourced operations.
B. The SITE/SICE's beneficiary or customer data or investment portfolio details and transaction data of assets under management shall be clearly segregated from the data of the service provider and of other institutions.
C. The SITE/SICE's beneficiary or customer data or investment portfolio details and transaction data of assets under management processed by the service provider shall be readily provided to the competent authority and the SITE/SICE when needed.
4. The SITE/SICE shall adopt a risk-based approach to conduct regular and unscheduled audits and to monitor the use, processing, and control by the service provider of beneficiary or customer data or investment portfolio details and transaction data of assets under management. External auditors may be engaged to conduct relevant audits.
5. When the foreign competent financial authority where the service provider is located requests for provision of information of Taiwan customers or beneficiaries, the SITE/SICE shall inform and obtain consent from the Taiwan competent authority in advance before such information may be provided.
Audits under subparagraph 4 of the preceding paragraph also may be delegated to the auditing unit or other relevant unit of another member enterprise of the SITE/SICE's business group. That auditing unit or other relevant unit furthermore shall provide the relevant audit reports to the SITE/SICE.
Point 12
If any outsourcing arrangement by a SITE/SICE will involve offshore processing of any operations deemed material relating to beneficiary or customer data or investment portfolio details and transaction data of assets under management, the SITE/SICE shall apply to the competent authority for approval, submitting the following documents:
1. The internal outsourcing rules adopted in accordance with Point 4, paragraph 2.
2. Meeting minutes containing a resolution of the board of directors.
3. Necessity and legal compliance analysis of the outsourcing of business operations, including an evaluation of the service provider's compliance with the beneficiary or customer data protection laws and regulations of Taiwan.
4. Outsourcing plan, which shall include the following contents:
A. Risk assessment and management mechanisms:
a. Evaluation of the risk level and materiality of the outsourced operations and the impact on business operations and beneficiary or customers interests.
b. Due diligence check of the service provider to ensure the reliability and legal compliance of the services provided; the reliability check shall include analysis of business continuity, substitutability, and

concentration.
c. Description showing adequate expertise and resources to monitor the service provider's execution of the outsourced operations.
d. Day-to-day monitoring plans and implementation units.
B. Description of beneficiary or customer data protection measures and whether beneficiary or customer consents have been obtained to ensure the quality of outsourced services and the protection of beneficiary or customer interests.
C. Information security and management:
a. Description of data security management measures, data transmission and segregation, and data ownership.
b. Description of management policies with regard to the locations of data storage, including assessment of legal, political, and economic stability at the data processing and storage locations, and description of data backup and data accessibility at any time.
D. Emergency response plans, including operational contingency plans that address circumstances in which the service provider is unable to provide service or the service is disrupted.
5. Letter of consent or outsourcing agreement signed by the service provider, agreeing that when necessary a person designated by the SITE/SICE may carry out auditing of the outsourced activities. An aforesaid designated person also may be assigned by the Taiwan competent authority at the expense of the SITE/SICE.
6. A statement issued by the service provider certifying that it has not had any occurrence of incidents such as employee fraud, information security breach, or other incidents damaging beneficiary or customer interests or undermining sound operations in the last three years.
When conducting outsourcing under the preceding paragraph, a SITE/SICE shall comply with the following provisions in addition to the preceding point:
1. It shall ensure that the use, processing and management of beneficiary or customer information by the service provider comply with Taiwan's Personal Data Protection Act, retain complete audit trails, and include these compliance matter in key audit items.
2. It shall periodically evaluate cost-benefit and the reasonableness of expense allocation within the group and submit the report to the board of directors for approval.
3. The standards for information system security testing shall be no less rigorous than the requirements set forth by the competent authority or the Securities Investment Trust & Consulting Association of the R.O.C. (SITCA).
4. It shall conduct one routine audit and one special audit at least annually, and shall submit the offshore outsourcing audit reports for the current year to the board of directors within four months after the end of each year. The aforementioned audits may be performed by an independent third party specializing in information technology.
5. It shall establish operational contingency plans that address circumstances in which the service provider is unable to provide the service or the service is disrupted.
6. It shall specify in the outsourcing agreement, with respect to any circumstance in which an outsourced service is transferred to another service provider or transferred back to the original enterprise, the service provider's obligations regarding system migration and handling of data, as well as the service provider's liability for damages in case of service disruption.
Audits under subparagraph 4 of the preceding paragraph also may be delegated to the auditing unit or other relevant unit of another member of the SITE/SICE's business group. That auditing unit or other relevant unit furthermore shall provide the relevant audit reports to the SITE/SICE.
Point 13
A SITE/SICE shall comply with the following rules when its outsourced operations involve cloud-based services:
1. It shall formulate policies and principles for using cloud-based services, adopt appropriate risk control measures, and heed the proper diversification of operations outsourcing to cloud service providers.
2. The SITE/SICE is ultimately responsible for the monitoring of cloud service providers and it shall have the expertise and resources to

supervise the cloud service providers' execution of outsourced operations. It may also request professional third parties to assist in monitoring operations as needed.
3. When the SITE/SICE, at its sole discretion, or in conjunction with another member of its business group, or in conjunction with other SITEs/SICEs that outsource to the same cloud service provider, appoints an independent third party with expertise in information technology to conduct auditing, the following provisions shall be complied with:
A. The SITE/SICE shall ensure that the audit scope includes important systems and control measures related to the operations outsourced to the cloud service provider.
B. The SITE/SICE shall evaluate the suitability of the third party and verify that the contents of an audit report submitted by a third party meet the relevant international standards of information security and privacy rights protection.
C. The third party shall conduct the auditing based on the scope of the operations outsourced by the SITE/SICE and issue an audit report.
4. When the SITE/SICE transmits and stores beneficiary or customer data or investment portfolio details and transaction data of assets under management at a cloud service provider, it shall adopt data encryption, tokenization, or other effective protection measures and it shall also establish appropriate encryption key management mechanisms.
5. The SITE/SICE shall retain complete ownership of data outsourced to cloud service providers for processing. The SITE/SICE shall ensure that the cloud service provider does not have the authority to access beneficiary or customer data or investment portfolio details and transaction data of assets under management except for the execution of the outsourced operations and it may not use the data for purposes outside the scope of the outsourced operations.
6. With respect to the processing by cloud service providers of beneficiary or customer data or investment portfolio details and transaction data of assets under management, and the data storage locations, the following rules shall be observed:
A. The SITE/SICE must retain the right to designate the location for the processing and storage of the data.
B. The local data protection laws and regulations at the offshore location shall be no less rigorous than the requirements in Taiwan.
C. Where deemed material, beneficiary or customer data or investment portfolio details and transaction data of assets under management shall be stored in a location within Taiwan in principle. If located offshore, unless otherwise approved by the competent authority, backups shall be retained in Taiwan of the important data of beneficiaries or customers or investment portfolio details and transaction data of assets under management.
Point 14
When a SITE/SICE outsources the development and maintenance of onshore information systems to offshore institutions, the preceding three points shall not apply.
Point 15
When outsourcing operations, a SITE/SICE shall not violate any mandatory or prohibitive provisions, public order or good morals, and there shall not be any adverse impact on its business operations, management, or the interests of its beneficiaries or customers. A SITE/SICE shall also ensure compliance with the provisions of securities and futures related laws and regulations, including but not limited to the Securities Investment Trust and Consulting Act, Money Laundering Control Act, Personal Data Protection Act, Financial Consumer Protection Act, Trade Secrets Act, and other applicable laws and regulations.
When outsourcing operations, a SITE/SICE shall vigorously observe applicable laws and regulations and the business rules or self-regulatory agreements set forth by the SITCA.
Point 16
With respect to operations outsourcing by a SITE/SICE, when the competent authority, SITCA, or appropriate institutions or personnel engaged by them conduct financial examination or auditing on the outsourced operations, the expense shall be borne by the SITE/SICE.

	If a service provider violates these Directions or other laws and regulations, the competent authority may, depending on the severity of the case, instruct the outsourcing SITE/SICE to terminate the outsourcing arrangement pursuant to the outsourcing agreement, request the service provider to make improvement within a given period of time, or suspend the outsourcing arrangement until improvement made by the service provider is confirmed. Point 17 Unless otherwise provided in these Directions, a SITE/SICE shall bring its existing outsourcing activities that do not conform to the provisions herein into compliance with these Directions within one year following the issuance and implementation these Directions.