**MIR 2.15.4(l)**

**Details of information technology systems and of arrangements for their supply, management, maintenance and upgrading, and security.**

**TABLE OF CONTENTS**

[1 Organisational System 1](#_Toc512514638)

[1.1 Principal Responsibility 1](#_Toc512514639)

[2 System Solution 2](#_Toc512514640)

[2.1 Logical Architecture 2](#_Toc512514641)

[2.2 Application Architecture 5](#_Toc512514642)

[2.2.1 Application Design 5](#_Toc512514643)

[2.2.2 High Availability 5](#_Toc512514644)

[2.2.3 Security 6](#_Toc512514645)

[2.2.4 Flexibility 6](#_Toc512514646)

[2.2.5 Scalability 7](#_Toc512514647)

[2.3 Disaster Recovery/Business Continuity 7](#_Toc512514648)

[3 Data Centre Construction Plan 10](#_Toc512514649)

[3.1 Layout Plan 10](#_Toc512514650)

[3.2 Network Facilities 11](#_Toc512514651)

[3.3 System Hardware 11](#_Toc512514652)

[4 Data Management 11](#_Toc512514653)

[4.1 Data Storage 11](#_Toc512514654)

[4.2 Data Backup 11](#_Toc512514655)

[5 Operation and Maintenance Management 12](#_Toc512514656)

[5.1 Operation and Maintenance Management 12](#_Toc512514657)

[5.1.1 IT Service Management 12](#_Toc512514658)

[5.1.2 Supply Management 13](#_Toc512514659)

[5.1.3 Incident Management 15](#_Toc512514660)

[5.1.4 Regular Maintenance 16](#_Toc512514661)

[5.1.5 Continuity 17](#_Toc512514662)

[5.1.6 Availability 20](#_Toc512514663)

[5.1.7 Ability 21](#_Toc512514664)

[5.1.8 Modification and Upgrading 22](#_Toc512514665)

[5.1.9 Data Backup 24](#_Toc512514666)

[5.1.10 Internal Audit 26](#_Toc512514667)

[5.2 Emergency 27](#_Toc512514668)

[5.2.1 Overview 27](#_Toc512514669)

[5.2.2 IT Emergency Plan 27](#_Toc512514670)

[5.2.3 Emergency Drill 29](#_Toc512514671)

[5.3 Security 30](#_Toc512514672)

[5.3.1 Information Security Process 30](#_Toc512514673)

[5.3.2 Data Access Control Process 30](#_Toc512514674)

[5.3.2.1 Data Security Defense 30](#_Toc512514675)

[5.3.2.2 Strategies for Data Access Control 31](#_Toc512514676)

[5.3.2.3 Data Destruction 32](#_Toc512514677)

[5.3.3 System Access Control Process 32](#_Toc512514678)

[5.3.3.1 Network Access 32](#_Toc512514679)

[5.3.3.2 Account and Authority 33](#_Toc512514680)

[5.3.3.3 Password Management 33](#_Toc512514681)

[5.3.3.4 User Action Audit 33](#_Toc512514682)

[5.3.4 Bug Scanning Process 34](#_Toc512514683)

# Organisational System

## Principal Responsibility

Responsible for cutting-edge research and technology introduction of the IT system; formulate IT strategy and system construction plan, coordinate IT system construction tasks; organize annual technological project planning, supervise the implementation of technological projects; information security system planning, establish and improve information security strategy; planning, design, maintenance of the information platform; overall implementation management of the Exchange’s business data; trade information resources procurement and in-house information services, exchange market conditions with other exchanges; official website planning and day-to-day operation and management.



The technology department is headed by CTO, with Development Manager, Test Manager, Project Manager, Product Manager and Maintenance Manager who report to CTO. The Development Manager is responsible for the management of the development team and the development of core system; the Test Manager is responsible for the management of the test team and system testing; the Maintenance Manager is responsible for the management of the maintenance team and the day-to-day operation and maintenance; the Project Manager is responsible for system development management to guarantee delivery; the Product Manager is responsible for product planning, design and product life-cycle management.

# System Solution

## Logical Architecture

Digital Cash Exchange System (hereinafter referred to as “DCES”) is a fully integrated and preeminent electronic trading and clearing platform, providing real-time service at its best to market participants. It offers a fast, reliable and efficient way for processing transactions for trading and clearing. Reliability, high availability and performance are extremely important to DCES. The system is robust, inherently stable and highly reliable, supports business continuity and avoids data loss or user interruption. In addition, DCES also has high performance in terms of processing power, system capacity, etc… It is able to accommodate continued growth in transaction volume too. .

DCES’s system architecture is fitted with the following components:

1. Trading Service

The trading system is the heart of the Exchange’s systems. It receives all orders, performs order validation, order book management, order matching and trade reporting. The trading service provided by DCES supports the corresponding business model of the Exchange. At the same time, the framework of the trading service is adaptable and does not require major changes to the code even if there is a change in the trading process of the DCES due to changes in the business.

1. Trading Business Management

The information of market participant (member, investor, bank, market data providers) is registered with the clearing house. Should each entity wish to participate in trading, they need to go through certain channels and entered their information to the trading system. The trading business management system is designed for the afore-said function and realizes pre-trade, in-trade and post-trade data exchange. Meanwhile, all basic trading data and status such as the exchange traded products, contracts and properties of contract are managed by this system.

1. Clearing Service

The clearing service provides clearing members with the ability to clear and settle trades, with on-line and real-time interfaces to the Clearing Banks. It supports the corresponding business model of the Clearing House.

1. Market Participant Management

Based on the Exchange’s corresponding business model, there is a variety of entities including member, investor, bank and market data provider participating in this market and these entities are collectively named as “market participant”. DCES need to record these participants’ information and designate their roles and privileges to facilitate their participation in the electronic market. The market participant management service is designed for the afore-said function.

1. In/Out Fund Management Service

In/Out fund Management Service provides fund transfer between bank account and trading account.

1. Forced Liquidation

Where a member fails to satisfy the margin call or holds excessive positions beyond the position limit, the exchange will implement forced liquidation to close out the member’s positions. Forced liquidation is a mandatory measure designed to prevent extension risk and shall be taken in a prudent manner.

1. Risk Control Service

Risk Control is designed to reveal the source of risk by monitoring market fund, position held, order entry and price trend. It adopts quantitative analysis to predict the probability and level of risk pooling, realises risk alert, risk source check and risk level analysis. Risk Control necessarily guarantees market stability and provides investors a fair and open investment environment.

1. Surveillance Service

When members and investors violate market rules and regulations, the surveillance system will detect and identify these behaviors and generate warning messages so that supervisors can make the necessary market intervention in these acts. Regulatory services support the corresponding business model of the Exchange and have the flexibility to integrate new products and define the corresponding regulatory rules for newly listed products.

1. Market Data Dissemination

This component handles management of market data distribution. When a trade is executed, the trading record and new “market picture” will be sent to market participants. When the settlement is done, given a clearing-to-member business model, the result of the clearing shall also be sent to members. DCES provides a prioritized mechanism for market data distribution. For the effectiveness of controlling network load, the frequency and depth of market data distribution are configurable.

1. Transaction Security Service

The Transaction Security Service manages transaction security handling and all encrypted functionalities such as PIN confirmation and message verification, etc.

1. Authentication Service

The Authentication Service is designed to manage the identification of market participants and provide single-point login and unified authentication for DCES’s subsystems.

1. Time Service

Time Service is a server for time management service that it controls the synchronized time between all the disparate systems.

1. Host Access Service

The core systems of the Exchange and the Clearing House should be in an internally safe network environment. Therefore, direct access to these systems from external member systems is not permitted. The exchange provides its members with host access service whereby the member system will be enabled to enter business messages including order entry to the front server of the exchange based on a pre-negotiated communication protocol between the Exchange and the member. Such message will be sent to the exchange’s internal core system after verified.

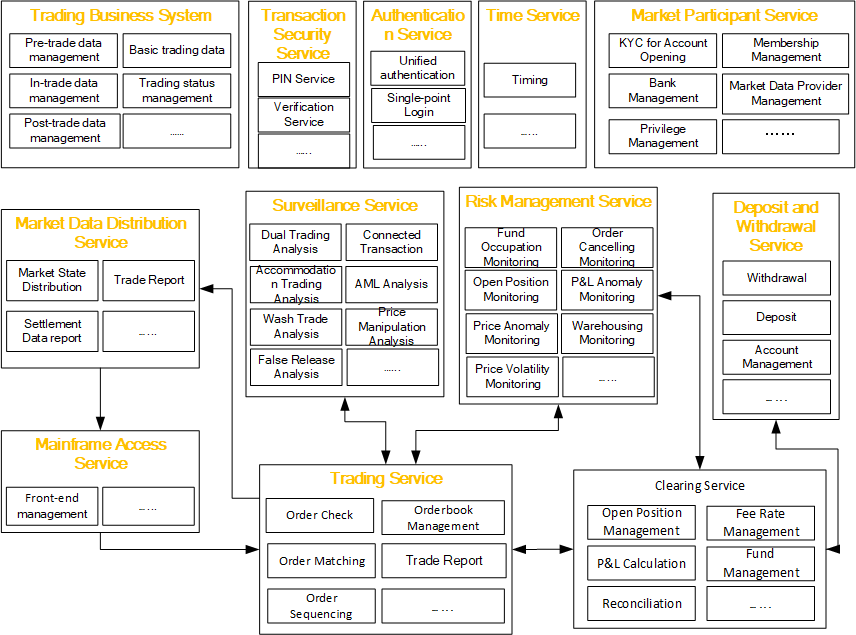


Figure 2‑1 Logical Architecture

## Application Architecture

The DCES application architecture takes a component-based architectural model that can be deployed separately or easily integrated. Components exchange information through standard communication protocols and interactive interfaces.

### Application Design

DCES application design is based on open architecture and multi-tier C/S model. Open architecture gives member companies the flexibility to integrate their front-end/back-end transaction and risk management systems. The multi-tier C/S architecture consists of service layers and functions that provide different levels of service. Trading, risk control, monitoring and other systems requiring higher real-time requirements, adopt the C/S model.

DCES supports “transaction replay” based on processing transaction flow. This function can be used not only for back testing and transaction rules verification, but also for improving system resilience. In addition, regulators can also traverse a sequence of events on a trading day to conduct a more accurate analysis of all types of trading.

### High Availability

DCES can provide near 7/24 trade to promote high availability electronic market and cross-border trading services , while the real-time processing capabilities of clearing services can also be adapted to the time window restrictions of transaction and post-trade clearing. System maintenance and end of day processing are minimized during the designing session. The high availability of DCES is principally achieved through the high availability of hardware and software. DCES supports component redundancy/mirroring with parallel processing. This mechanism achieves high availability by eliminating a single point of failure.

All transactions, changes in market state, and changes in trading status are persistent to survive transient failures of the host systems. By the “sequencing and replay”’ mechanism, things can be rebuilt in the order they were before the error occurred. Through reliable UDP broadcast protocol, the information can be copied to the backup host system in real time. Each fault-tolerant component has the same content as the principal component. Once the principal component fails, the backup component can immediately take over the task and continue to run, to ensure that business processes are not affected. In our design, the principal and backup components remain in the same state.

System hardware and software requirements can automatically recover from a single point of failure without manual intervention. In addition, each system can transfer processing tasks to other nodes/processors in the event of a failure.

### Security

Security is a vital and integral part of the architectural design of DCES. Security measures are indeed critically important to the distributed technology model. A good security measure and its associated security policy will ensure system security to keep unlawful intruders at bay.

Below are the security considerations in designing DCES:

1. ID Authentication

ID authentication is a kind of security policy, the policy through some certain technical means, to confirm the user permissions, in order to ensure that the user to send messages, receive messages, or access to the system to identify its identity and limit its authority. Each user has his or her corresponding access rights. The user only allows access to the trusted target within the permission, and does not allow unauthorized access to the data. Every visit will leave a mark to ensure the audits.

1. Message Privacy

Each user has a corresponding private key, and all messages sent and received by the user will be encrypted and decrypted by the private key. Even if an unauthorised individual intercepts the message, they cannot access the message content.

1. Message integrity

Messages cannot be tampered with. Message Integrity is to ensure that the sender and receiver of the transaction are able to know that the message they viewed matches the message sent by the other party.

1. Non-repudiation

The source of the message can be determined and then sender of the message will be prevented in denying the message that has been sent.

DCES uses industry-leading security standards to establish a security framework that ensures transaction security through the adoption of rigorous identification methods and leading cryptography. All users need to be identified before they can interact with the system. Only authorized individuals or groups can access the exchange’s system, and all network devices need to be verified before they are received.

### Flexibility

DCES can support multiple markets, multiple currencies and multi-trading timetable. DCES provides an extensible, rule-based trading framework to support different market structures with different trading rules. Trading rules are made in a variety of templates, for example, position limit templates, trading timetable templates, etc. to meet rapidly changing business development and functional needs and provide support for the clearing function.

DCES provides flexibility to control the market, the trading and clearing phases automatically or manually.

DCES allows its services to be accessed from a variety of locations across multiple devices.

### Scalability

The design of DCES takes into account system scalability. The system design must be robust enough to handle the huge volume of trading. At the same time, the capability of the system to handle transactions can achieve linear growth by adding new components or nodes. Trading and clearing systems handle the average, peak and special volume of transaction increases, and system performance does not deteriorate with volume growth.

## Disaster Recovery/Business Continuity

Trading and clearing environments are of paramount importance to the Exchange and the Clearing House. Such a mission critical operating environment should be able to ensure continuous operation around the clock. However, the disaster situation cannot be completely ruled out. In the event of a disaster, the interruption to the key operating environment must keep to minimal and should be resumed in the shortest time. DCES employs multiple disaster recovery strategies at multiple levels. At the system level, the highest priority for business continuity trading system, including the cluster strategies: the master-slave mode, the parallel redundancy mode, the load balance mode, to build highly available system architecture. Among them, the front-end cluster with load balance mode, is responsible for receiving the delegate and entrust members to deal with the situation sent to members; compositor cluster using the master-slave mode, is responsible for sequencing the orders by the receipt sequence number and persistence; when there is a major system failure requesting system restart, the sequenced orders can be read and replayed according to trading rules to restore the transaction to the pre-fault state. When the sequenced orders enter the matching engine cluster, the cluster will adopt the parallel redundancy mode. Multiple matching engine cores will simultaneously match the orders and generate information of trade report and market state.



**Figure 2‑2** Principal Centre Trading System High Availability Design

Logically speaking, Disaster recovery centre is a replica of the principal centre. To remain the same state as the principal centre, the disaster recovery centre will need the principal centre to transmit necessary information via the network. For an order-driven trading system, the disaster recovery centre with good connectivity can directly copy the orders and the trade-report messages received by the principal centre. The logical relationship between the principal centre and disaster recovery centre is shown in the flowchart below.



**Figure 2‑3** Disaster Recovery Logic Topological Graph

In the design of the trading system, the backup centre receives the sequenced orders of the principal centre as the principal centre does. When the principal centre fails over, the backup centre can take over the work of the principal centre at any time to ensure that transaction processing is not interrupted and the data is not lost. In terms of architecture, as far as the backup centre is concerned and as long as the trading system is extended on the bus and directly accesses to the principal centre, it can receive order entry and trade report from the principal centre.



**Figure 2‑4** the Highly Available Design of the Trading System for Local and Remote Disaster Recovery Centres

# Data Centre Construction Plan

## Layout Plan



**Figure 3‑5** the logical topology of the Exchange

The data centre is deployed in the UAE, the regulator can obtain required transaction data through the API interface of the trading system.

The principal centre will be deployed in Abu Dhabi, the backup centre will be deployed in Dubai. Both data centre will meet business and regulatory requirements.

## Network Facilities

The Exchange and the Clearing House completes order routing, execution reporting and clearing and settlement activities by establishing a core private network that meets the business requirements of trade, clearing and other services in terms of capacity, speed, security and reliability. The principal network adopts the traditional 3-layer network structure, the backbone network bandwidth is 10GB and the access bandwidth is 1GB.

Members can send their orders to the Exchange through the Internet or VPN and receive the corresponding response from the Exchange. The orders need to enter the front server provided by the Exchange first, and then entered the private system for processing after authentication and verification.

## System Hardware

Each subsystem of the Exchange and Clearing House consists of multiple servers, which consist of a distributed cluster consisting of physical machine and virtual machine. Data is stored on disk arrays of database, and system history data can be stored on tape drives.

# Data Management

## Data Storage

There is a large number of critical data stored in the exchange’s system and therefore data security is a primary consideration of DCES. High-speed networked storage devices like SANs are employed for data storage. For database, mainstream products from vendors like Oracle can be used and system reliability can be enhanced via operation modes like RAC. In addition, massive business data such as trading flow is stored as a file. For these data, we can use conventional methods such as RAID preservation. At the same time, to balance performance and storage efficiency, business data can be segmented and rapidly growing data can be stored separately over time. For data storage, fault tolerance and no single point of failure are necessary and the provision of a central tape library backup facility is preferred.

## Data Backup

According to data classification and characteristics, the technology department formulates the backup strategies, including daily backup, special day backup, version-upgrade backup and the shelf life, backup mode, backup media, data cleaning cycle of various types of data.

Details are available in Section 5.1.9 Data Backup

# Operation and Maintenance Management

## Operation and Maintenance Management

### IT Service Management

The technology department is committed to providing the Exchange and the Clearing House with safe, stable and efficient operation and maintenance services. In order to improve the quality of operation and maintenance services and standardise operation and maintenance management, there is an IT service management system set in place.

This document is a programmatic document for the IT service management system and specifies the objectives, management mechanism and requirements of the system.

Through the establishment of a sound IT service system, continuing efforts will be made in operation and maintenance management, emergency and security and to raise the bar of IT service management, guarantee security, stability and efficiency of operation and management and enhance the corporation’s core competency.

The IT service management system is composed of Service, Process and Audit. Through an integrated mechanism for supervision, review, verify, report and improvement, systematic continuous improvement is ensured. The well-functioning system is such that all IT services it renders comply with the requirements to the satisfaction of various parties including market, business, audit and the Regulator and security and quality of such service is ensured at all times and work efficiency is demonstrated with technological advances.

1. Service describes the IT services provided by the IT function and displays the service categories.
2. Process is through the entire work flow provided by the service and solves the “how to” problem.
3. Audit is supervised and audited by internal personnel to ensure that the work process of the IT function meets the expected standards.

Through the above service management structure, the technology department will accurately and reasonably analyse and categorise requirements from market, business, audit and the Regulator, realise compliance and controllability of the IT services and continue exploration and optimisation to provide secure, stable and efficient IT services for the Exchange and the Clearing House.

The IT services are described as below:



The following documents will be generated under this section:

|  |  |
| --- | --- |
| Item | Summary |
| IT Service Management | Overview of the entire operation and maintenance system |
| Characters of IT Service Management | Details about the roles and responsibilities of the process and system |
| Service List | Description of the services of the data centre |
| Meeting List | Descriptions of meetings held on a periodic basis |

### Supply Management

The technology department manages IT service suppliers. It strengthens the supervision of the service process by establishing a supplier management flow and ensures that the quality of the products and services provided by such supplier satisfy the requirements of the Exchange and the Clearing House.

There are Supplier Manager, Supplier Linkman, Supplier Management Team under the technology department to ensure a well-functioning management flow. The responsibilities of the preceding functions are:

1. Supplier Manager: flow management, prepare and maintain the supplier list and contract list; performance evaluation
2. Supplier Linkman: cooperation in performance evaluation; supplier supervision
3. Supplier Management Team: annual supplier evaluation; advice on the evaluation

There are important and ordinary suppliers rated as below:

|  |  |  |
| --- | --- | --- |
| Level | Description | Standards |
| Important | Suppliers providing products and services for trading and clearing systems | Qualified with 4 points on average (5 points the highest) |
| Ordinary | Suppliers providing products and services for “unimportant” purposes such as operational support, etc. | Qualified with 3 points on average (5 points the highest) |

The aforesaid points are given on the following bases:

|  |  |
| --- | --- |
| Execution | Delivery result; execution progress; product quality; after-sales and technical support; training; others |
| Support | Service attitude; demonstrated professionalism; pro-active communication, etc. |

The following documents will be generated under this section:

|  |  |
| --- | --- |
| Item | Summary |
| Supply Management | Overview of the external supplier management system |
| Supplier List | Supplier list |
| Contract List | Service contract list provided by suppliers |
| Supplier Evaluation | Annual supplier evaluation to determine supplier level |

### Incident Management

The technology department reasonably defines the levels of plausible incidents, regulates the handling process, quickly and effectively resolves all incidents, minimises the incidental impact and ensures normality of business operation.

Incident Manager is mainly responsible for:

1. Designing and improving of incident management processes;
2. Setting up performance indicators for event management
3. Co-ordinating resources and facilitating resolution;
4. Tracking and monitoring incident circulation;
5. Collecting and summarising flow-related information and preparing management reports;

All incidents are categorised into software, hardware, infrastructure environment, security, consultation, service requirement, technical support and rated as either **Impact Degree or Emergency Degree:**

| **Impact Degree** | **Description** |
| --- | --- |
| High | Impact many members and may cause material losses to them. |
| Medium | Impact several members and may cause certain losses to them. |
| Low | Hardly any impact on any member. |
| **Emergency Degree** | **Description** |
| High | Impact or may impact real-time operation (trading, bid and offer, risk control, surveillance) and must be immediately executed or resolved without delay. |
| Medium | Have undiscovered danger that may impact real-time operation (trading, bid and offer, risk control, surveillance) but can be resolved following market close as authorised;  Outside normal trading hours, impacted non-real-time operation such as settlement required by members. |
| Low | Outside normal trading hours, with undiscovered danger that may impact operation but not require immediate resolution;  Relating to service requirement. |

All incidents are quantified according to impact and emergency:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Priority** | | **Impact Degree** | | |
| High | Medium | Low |
| **Emergency Degree** | High | 1 | 1 | 2 |
| Medium | 2 | 3 | 4 |
| Low | 3 | 4 | 4 |

The incident-degree-led response mechanism:

| **Priority** | **Time of Response** | **Time of Resolution** |
| --- | --- | --- |
| 1 | Immediate (in 5 minutes) | 30 minutes |
| 2 | 30 minutes | 4 hours |
| 3 | 2 hours | 12 hours |
| 4 | 4 hours | 48 hours |

The following documents will be generated under this section:

|  |  |
| --- | --- |
| Item | Summary |
| Incident Management Process | Overview of incident management process and incident definitions |
| Incident Classification Table | Known incidents listing |
| Incident Priority | Known incident rating to determine which level of resolution shall apply |

### Regular Maintenance

In order to establish an efficient and reasonable operation and maintenance process, the technology department has formulated specifications for daily operation and maintenance and illustrated commonly used commands and methods for regular maintenance of the network, host, and application, directing operation and maintenance personnel and further ensuring the security, stability and reliability in monitoring and maintaining the operation.

The following documents will be generated under this section:

|  |  |
| --- | --- |
| Item | Summary |
| Regular Maintenance Process | Description of regular operation and supervision processes |
| Maintenance Manual for Infrastructure Environment | - |
| Maintenance Manual for Network | - |
| Maintenance Manual for Firewalls | - |
| Maintenance Manual for Host | - |
| Maintenance Manual for Application | - |

### Continuity

This process is designed to ensure that the Exchange and the Clearing House meet the requirements of providing critical operations and services as a going concern in the event of a disaster or other major incidents:

1. Business disruption (e.g. failure of IT services) will be resolved within a defined time frame;
2. Normality will be duly and efficiently restored following the result of any significant and adverse impact.

Continuity Manager is mainly responsible for:

1. Writing and revising relevant documents;
2. Training on relevant systems and process documentation;
3. Establishing continuity management indicators and evaluate them;
4. Organising business impact analysis and continuity risk assessment;
5. Organising and formulating emergency response plans at the departmental level and supverising emergency response drills

According to the degree of business impact (B) and the probability of threat occurrence (P), the incidents are categorised and quantified:

|  |  |  |
| --- | --- | --- |
| **Probability of Threat (P)** | | |
| **Level** | **Value** | **Description** |
| High | 5 | Most likely to occur or previously occurred for many or a number of times and the occurrence rate is on the rise |
| Medium | 3 | Previously occurred or despite never occurs, may occur if without appropriate management. |
| Low | 1 | Seldom occurred in the past or unlikely to occur under appropriate management |
| **Business Impact (B)** | | |
| **Level** | **Value** | **Description** |
| High | 5 | As a result of business security damage, core operations may be disrupted, activities related to the business may be adversely impacted, the reputation and financial resources of the Exchange may be damaged. |
| Medium | 3 | As a result of business security damage, major operations may be disrupted and certain losses may be caused. |
| Low | 1 | As a result of business security damage, irregular operations may be caused with minor losses. |
| **Risk Degree R=P×B, threshold for formulating the emergency plan: R≥9 or B=5** | | |

Relevant emergency plans will be made according to the above principle. (Details are available in Section 5.2.2 IT Emergency Plan)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Number** | **Disaster and Failure** | **Probability of Threat (P)** | **Business Impact （B）** | **Risk Degree （R）** | **Emergency Plan** |
| 1 | Infrastructure Environment | 1 | 5 | 5 | Emergency Plan for Infrastructure Environment |
| 2 | Power supply system failure | 3 | 5 | 15 |
| 3 | Internal power system failure | 1 | 5 | 5 |
| 4 | A/C system failure | 3 | 1 | 3 |
| 5 | Monitoring system failure | 1 | 1 | 1 |
| 6 | Telecom network failure | 3 | 1 | 3 | N/A |
| 7 | Core network failure | 3 | 5 | 15 | Emergency Plan for Network |
| 8 | Firewalls failure | 1 | 5 | 5 |
| 9 | Server and OS failure | 3 | 5 | 15 | Emergency Plan for System And Application |
| 10 | Trading system failure | 3 | 5 | 15 |
| 11 | Clearing or risk system failure | 3 | 5 | 15 |
| 12 | Principal centre failure | 1 | 5 | 5 | Emergency Plan for Principal-Backup Centre Switching |
| 13 | Virus | 3 | 3 | 9 | Emergency Plan for Information Security |
| 14 | Network attack | 1 | 3 | 3 |
| 15 | Fire disaster | 1 | 5 | 5 | Emergency Plan for Disaster |
| 16 | Earthquake, tsunami | 1 | 5 | 5 |
| 17 | Events | 1 | 5 | 5 | Events Guide |

In addition to emergency plans, the technology department will formulate drill plans that set out drill objective, performers and responsibilities, drill arrangements, plans, schemes and procedures for the further guarantee of the critical operations and services of the Exchange and the Clearing House as a going concern. An emergency drill (involving relevant departments, suppliers and member) will be held every year to discover potential impact and threat that the Company’s IT system may be exposed to and relevant reports will be made after the drill. (Details are available in Section 5.2.3 Emergency Drill.)

The following documents will be generated under this section:

|  |  |
| --- | --- |
| Item | Summary |
| Continuity Process | Introduction and description of the continuity management process |
| Business Impact Analysis and Continuity Risk Assessment | Evaluate and rate known risks |
| Emergency Plan | Refer to 5.2 Emergency |

### Availability

The technology department develops the availability management of IT infrastructure, network and application systems and pays attention to the duration of each interruption and the total duration of interruptions. This ensures that the availability of IT services continues to comply with regulatory requirements and effectively meet business needs.

Availability Manager and Availability Administrator are responsible for:

1. Availability Manage: Designing and improving the availability management process; setting performance indicators for availability and assessing the performance; collecting availability needs, formulating availability objectives; formulating, maintaining and implementing availability plans; collecting and aggregating execution information, reporting problems arising from execution, providing improvement proposals and making improvement plans.
2. Availability Administrator: IT services availability planning within the scope of responsibility; providing availability data; writing availability management reports.

An availability incident refers to any incident resulting in IT services failure or overall system interruption as a result of disruption, downtime, etc. The following incidents shall be regarded as an availability incident:

1. The breakdown of power supply, air conditioning, video surveillance and infrastructure monitoring of the server room and no automatic recovery occurs in the next one minute.
2. Business disruption as a result of the breakdown of the internal network, any equipment of the host, firewall and/or database of the Exchange and/or the Clearing House and no automatic recovery occurs in the next one minute.
3. The disruption of the business systems including the trading system and the clearing system and no automatic recovery occurs in the next one minute.
4. The breakdown of the lines connected to the Internet and no automatic recovery occurs in the next one minute.

After a continuous incident occurs, the continuity administrator will keep a record and carry out reviews on a yearly basis.

Availability Manager formulates availability plan on a yearly basis and the statistical indicator applied is as below:

The following documents will be generated under this section:

|  |  |
| --- | --- |
| Item | Summary |
| Availability Process | Introduction and description of the availability management process |
| Availability Plan | Annual availability planning upon various systematic needs |
| Availability Calculations and Monitoring Table | Systematic availability records |

### Ability

The technology department regulates IT ability management to ensure rationality in the utilization of resources and services. Relevant ability thresholds are formulated in consistence with the needs of various business systems and the conditions of hardware and software and to ensure current and future business needs are and will be met to the extent appropriate and applicable.

Ability Manager and Ability Administrator are responsible for:

1. Ability Manager: Designing and improving the ability management process; set up ability management indicators; addressing ability management demand; formulating ability management objectives; collecting and aggregating execution results.
2. Ability Administrator: Executing the ability plans; monitoring and analysing ability incidents; reporting potential problems or tabling improvement proposals.

An ability incident refers to any incident impacting business operation as a result of ability or performance problems. The scope of surveillance includes infrastructure resources, network resources (CPU, bandwidth, etc.), storage, etc. Where there is an ability incident (such as excessive network traffic, device CPU exceeding the pre-determined threshold, etc.), the ability administrator will inform relevant specialists to upgrade capacity to meet future demand.

The following documents will be generated under this section:

|  |  |
| --- | --- |
| Item | Summary |
| Ability Management Process | Introduction and description of the ability management process |
| Ability Plan | Annual ability planning upon various systematic needs |
| Ability Statistical Table | Systematic ability records |

### Modification and Upgrading

This Section focuses on the management and control of modifications and upgrades of the services, software, hardware and infrastructure in the server room and relevant environment throughout day-to-day operation and maintenance; formulation of modification rules; standarisation of modification and upgrade processes of the operational centre; elimination or mitigation of risks that may arise from any modification; reduction of modification impact on operating and settling trades; and assurance of systematic security and stability. The key purpose of the aforesaid arrangements is to meet regulatory requirements in respect of software, hardware and system upgrade.

According to the impact and understanding of modification, the levels are set as below:

| **Modification Levels** | **Principle of Definition** |
| --- | --- |
| **Important Modification** | The following risk-based principles are applied for judgement:   1. Whether any modification is related to the core trading modules, technical architecture and core components; 2. The spread of influence on market participants as a result of implementation or failure of any modification; 3. Whether verified or not.   Details are available in *Modification Risk Assessment and Classification Table*. |
| **Medium Modification** |
| **Mini Modification** |
| **Standard Modification** | Small-scale modification that is made frequently with clear plans and may have known and de minimis risks that would not disrupt the services.  Such modification has been pre-authorised and can be reflected in the form of service requests. |

The process of modification shall have the following touchpoints:

1. Application submitting – application of modification submitted by an applicant
2. Formulation and evaluation of scheme – scheme formulated and evaluated by the applicant (modification of standards are available in *Guide to Standard Modification*, and other modification shall be subject to actual conditions on a case-by-case basis)
3. Audit – audit of a modification by relevant person in charge
4. Execution – execution of the audited modification by the applicant
5. Checking – check of the modification by a person who is not the applicant
6. Review – ex post review of the modification process by the applicant who shall continue to trace the modification
7. Close – close of modification by the applicant after the whole modification process is completed and review of such modification by person in charge

The following documents will be generated under this section:

|  |  |
| --- | --- |
| Item | Summary |
| Modification and Upgrading Management Process | Description of the upgrade and modification management process |
| Modification List | Definition of modification category and levels |
| Modification Risk Assessment and Classification Table | Description of modification-related risks |
| Standard Modification List | Specification of standard modification |
| Guide to Standard Modification | Operation manual of standard modification |

### Data Backup

Data backup strategies are formulated to enhance operational security of all information systems of the Company and ensure information integrity and consistence of the business system.

1. Data backup

In accordance with the importance of data, there are three security levels, i.e. high, medium and low. The backup strategies are as below:

|  |  |  |
| --- | --- | --- |
| Level | Data range | Backup strategies |
| High | Business data including member information, trading, settlement and risk management data, etc. | Daily incremental backup; weekly full backup; Daily and weekly backup to CD-ROM; relevant data media are simultaneously stored at the principal data centre and the disaster recovery centre |
| Medium | Operational and deployment information, work flows, sound recording and video monitoring and other internal data. | Weekly filing; weekly inspection of video data to confirm the storage of data generated in the previous ninety days |
| Low | Various notices | No backup |

1. Daily incremental backup
2. Daily incremental backup is exported as data pump and stored in compressed files.
3. Daily trading, risk management and bank turnover data are stored in compressed files.
4. Daily settlement statement for every client and surveillance logs are stored in compressed files.
5. Daily incremental backup of each set of system is recorded on CD-ROM which is made in duplicate with labels and to be kept in the CD cabinet.
6. Weekly full data backup
7. Weekly full data backup of each set of system is exported as data pump and stored in compressed files every Friday evening.
8. Client data are stored in compressed files every Friday evening.
9. Weekly full data backup of each set of system is recorded on CD-ROM every Friday evening; such CD-ROM is made in duplicate with labels and to be kept in the CD cabinet.
10. The full backup of historical query server database is exported as data pump and stored in compressed files every Friday evening.
11. Daily and weekly data backups and historical query server database full backup of each set of system are kept on file on hard disk by data/media administrator.
12. Data recovery
13. Back-to-back testing of recovery verification of incremental data in the database is conducted on a daily basis;
14. Back-to-back testing of recovery verification of full backups (CD-ROM and magnetic disks) of business data is conducted on a quarterly basis;
15. Spot tests of the full backup of a certain trading day in the production system will be recorded and the result of such test will be kept upon completion of the test.

The following documents will be generated under this section:

|  |  |
| --- | --- |
| Item | Summary |
| Data Backup Process | Description of the backup process for trading, settlement and other data |

### Internal Audit

An internal audit of the management system will be implemented to verify the effectiveness of the implementation of the management system and compliance with standard requirements, ensure compliance of day-to-day operation and maintenance, set out internal audit planning and implementation, prepare internal audit management reports, and track and verify corrective prevention implementation.

QA Manager and QA Administrator And Auditor are mainly responsible for:

1. QA Manager: Design and improve internal audit management processes; initiate and organise internal audits, appoint an internal audit leader and establish an internal audit team; review and supervise internal audit activities and internal audit reports;
2. QA Administrator: Prepare Internal Audit Inspection Form; formulate Internal Audit Plan; co-ordinate internal audit implementation;
3. Auditor: Internal audit plan implementation.

QA Manager shall appoint an internal audit leader and auditors subject to laws, regulations, regulatory requirements, management standards of the Company and shall carry out an internal audit on a yearly basis; the internal audit process is as below:

1. Plan of internal audit - QA Manager initiates an internal audit arrangement and the internal audit leader formulates the plan;
2. Opening meeting – The opening meeting shall be organized and presided by the internal audit leader and attended by heads of departments before the on-site audit is implemented; the leader shall introduce the purpose, scope, method and procedure and set out specific requirements and determine the timeline;
3. Audit - The internal auditor examines each item in accordance with the Internal Auditing Inspection Form and conduct audits by asking questions and reviewing documents. After the on-site audit, the internal audit team leader shall organise an internal exchange meeting to determine any non-compliant item;
4. Final meeting – The final meeting shall be presided by the internal audit leader and attended by QA Manager, internal auditor and heads of audited departments; the internal audit team shall introduce the audit result including without limitation: review of the audit, non-compliant item(s) and audit opinions, etc.
5. Internal audit report – The internal audit leader prepares the Internal Audit Report.
6. Continuous improvement – Service improvement and relevant documents writing based on the audit result.

The following documents will be generated under this section:

|  |  |
| --- | --- |
| Item | Summary |
| Internal Audit Management Process | Description of the internal audit process |
| Service Improvement Management Process | Description of the service improvement process and promoting service improvement |
| Service Improvement Management Report | Formation of the service improvement situation report |

## Emergency

### Overview

For the purpose of ensuring the requirements of providing critical operations and services as a going concern to be met, emergency manuals in relation to business operation and software and hardware systems are in place to prevent any problems beyond control and eliminate or mitigate any risk to the extent possible.

### IT Emergency Plan

Where any major emergency event occurs, the following process shall apply:

Principle - Upon receipt of an event report, first priority shall be placed on recovering business operation and minimising any disturbance to and any effect on the business;

Event Detection - On-site inspection tour, monitoring tools, client or internal fault reporting by operators on duty;

Reporting Process - Upon detection of any fault, the operator on duty shall notify the technician (i.e. person in charge on the site) to further confirm such detection and take either step in case of: (1) misinformation confirmed, the operator on duty shall be notified in a timely manner; (2) a major event confirmed, the head(s) of the functions involved, maintenance manager, event-related manager and event-impacted client(s);

Coordinating and Disposing - For any event that can be addressed with a pre-arranged emergency plan, the maintenance manager shall approve any measure to be taken in response to such event; absent an applicable plan, person in charge on the site shall make a temporary plan and submit it to the head of the operation and maintenance centre who shall make decisions to direct person in charge on the site for implementation.

1. Solving and Informing - Person in charge on the site should submit an application for modification in accordance with the temporary plan or solution for service recovery and is required to implement, record and review the whole process; the operator on duty shall record the result and time of handling the major event and notify event manager; at any time a major event is addressed, the operator on duty shall notify any party involved in such event.



|  |  |
| --- | --- |
| Item | Summary |
| Events Guide | The emergency handling process for reference in case of a major event |
| Events List | Event lists and indices of files and sections setting out emergency plans |
| Emergency Plan for Infrastructure Environment | - |
| Emergency Plan for Network | Including network equipment and firewall |
| Emergency Plan for System And Application | Including OS and application |
| Emergency Plan for Information Security | - |
| Emergency Plan for Disaster | - |
| Emergency Plan for Principal-Backup Centre Switching | - |

### Emergency Drill

In order to ensure the fault-tolerance capacity for the business and system and improve employees’ emergency response capability, the technology department is, in principle, responsible for the internal system drill and principal data centre and disaster recovery centre switch test on a yearly basis. Such drill is set to ensure that personnel involved in all touchpoints are fully mindful of the emergency process and their response capability will be improved.

The following documents will be generated under this section:

|  |  |
| --- | --- |
| Item | Summary |
| Emergency Drill for Network | Internal system drill |
| Emergency Drill for Application | Host and application system drill |
| Emergency Drill for Principal-Backup Centre Switching | principal data centre and disaster recovery centre switch test, member involved switch test |

## Security

### Information Security Process

In order to ensure effective information security in the IT service process and make business operations comply with relevant laws and regulations, the technology department has relevant security management systems in place to comply with the requirements to the satisfaction of the Regulator.

Information Security Manager and Information Security Administrator are responsible for:

1. Information Security Manager: Process design and improvement; process documentation update; organisation and implementation of risk assessment; tracking the resolution of information security incident; information security incident reports; training;
2. Information Security Administrator: System and service risk assessment; monitoring the effectiveness of security measures.

Information security management process:

Information requirements collection- formulation/improvement of security management system, norms and standards - formulation of risk assessment plans - formulation of risk disposal plans - implementation - security inspections and monitoring - statistics, grades and reports - formulation and implementation of improvement plans

### Data Access Control Process

With the establishment the Company’s data access control strategy, operational security of all information systems of the Company is enhanced and information confidentiality, integrity and availability of the business system are guaranteed.

#### Data Security Defense

1. Confidentiality: Important confidential files or data stored in the storage media and network transmission media should be encrypted to prevent data theft; papers with confidential data should be sealed and stored in a visible manner.
2. Integrity: Hardware faults of the devices where important confidential files or data are stored are monitored; the network conditions of the transmission networks of important confidential files or data are monitored; and the keys used for encryption and decryption are in strict custody. Version control or other non-repudiation processing should apply to the data with high integrity requirements in order to prevent malicious tampering; data in the production environment should not be modified directly and any such modification should be realised by tested or validated programme or script; data modification should be conducted, reviewed and approved through the modification management process.
3. Availability: Bugs in operating system and database system on devices are detected and cleaned on a regular basis. For example, periodic bug scan will select important patches for testing and installation; strictly access control is implemented for important confidential files or data storage devices (in order to meet the minimum authority required for work-related request); anti-virus and anti-trojan tools are used to prevent computers and other terminal equipment from being infected with malicious programs that may steal confidential data or system passwords; in the event that the information storage time is longer than the life cycle of the media for storage, another new media should be used for the continuation of storage; backup of important confidential documents or data is conducted on a regular basis.

#### Strategies for Data Access Control

External access:

1. Business data shall include client data and transaction, settlement, and risk control data and shall be treated as trade secrets that any unauthorised review, copy and transmission is strictly prohibited.
2. Inquiries and analyses of business data must be conducted at designated locations. It is forbidden to bring data privately out of the designated area.
3. Operation and maintenance data shall include system deployment information, work flows and other internal data. In case of any external access demand, the data access registration form should be filled out and be approved by head of the technology department in advance and the approved review shall be conducted in the custody of the system administrator.
4. Inquiries and analyses of operation and maintenance data should be done at designated locations. It is forbidden to bring data privately out of the designated area.

Internal access (mainly for the data requiring high-level security management):

1. Database access is controlled through database accounts which are divided into management account and application account.
2. Database account allocation requires approval of the account authority application form.
3. The database management account is only used for database management and must not be used for business operation and/or any business data modification.
4. The database application account is only used for application system operation, database changes and system emergency response and must not be used for any business data modification.

#### Data Destruction

1. It is forbidden to take away any discarded data and/or CD-ROM that should be destroyed in a crusher at the designated area.
2. Storage media (removable hard disk and USB flash drive) can only be used inside the designated place and must not be taken away outside such place. Any data stored there in should be deleted after used.
3. In order to ensure data security, any faults found in any media (removable hard disk and USB flash drive) containing sensitive information should be scrapped immediately.
4. if the storage medium (removable hard disk or USB flash disk) fails, it will be directly disposed of.
5. When any device is re-used, complete and irreversible clearance of the data stored therein must be ensured.

### System Access Control Process

#### Network Access

1. Internal and external networks are physically isolated through firewalls the devices of which are those meet international protection standards; Firewall policies, IDS and IPS devices are in place to monitor and intercept illegal intrusions and ensure the security of the internal systems of the Exchange and the Clearing House.
2. Networks for both trading and clearing are strictly isolated from other networks (such as for operation, management, testing, etc.)
3. The network access control policy is pursuant to the principle of least privilege and avoids over authorisation.
4. No terminal equipment is permitted to access internal networks unless satisfying authentication, authorisation and security check and monitoring to the extent that no virus or malicious code can intrude the internal networks and steal or destroy any significant and/or confidential information therein.
5. Remote management of servers and network devices cannot be effected without login through an encrypted tunnel which prevents data transmission from eavesdropping attacks.
6. Encryption is applied on client credentials that principally include username and password stored on internal servers.

#### Account and Authority

1. Set account authority for three account groups, i.e. ADMIN (read/write), VIEWER (read), and EMERAGENCY (read/write).
2. Only the VIEWER account is used for day-to-day operation; the ADMIN account is used after the change and upgrade of operation is approved; and the EMERAGENCY account is used after authorisation in case of emergency.
3. Based on the architecture applied by major financial institutions, account information is stored on ACS Server which controls and authenticates the access to such information.
4. The authorisation of user account authority shall satisfy the principle of least privilege and avoid over authorisation.
5. Access to the devices of the internal system is forbidden unless through a bastion host which keeps records of login and operation to meet regulatory or auditing requirements.
6. All applications and/or changes in account and authority must be approved and the records of such application and/or change must be kept;
7. Relevant account and authority changes shall be made in a timely manner to accord with the changes in the holder of the account;
8. Internal staff should avoid using super administrator account for day-to-day operation and prevent operational mistakes arising from the use of such account;
9. The authorisation of user account authority shall satisfy the principle of least privilege and
10. Employees are prohibited to divulge their account and passwords.

#### Password Management

1. Passwords must be set for all production environment system accounts;
2. The password must meet the complexity requirements: 1. Include at least three of the four: an uppercase character, an lowercase character, a number and/or a special character; 2. Password with a length the length of 10 characters and valid in the most recent six months is not permitted for re-use.
3. The password for every account must be updated at least every six months
4. The password for important system accounts must be updated every month.

#### User Action Audit

1. The function of recording logs should be enabled. Any user login through a bastion host to access network device, core system applications and conduct operations on the bastion host should generate audit records.
2. Effective measures (regular backup or authorisation control) should be taken to prevent deletion, modification or overwriting of audit records.

### Bug Scanning Process

By standardising bug scans, known bugs in the IT system are detected to form the basis of risk assessment.

New System Go-live Bug Scan - Information Security Administrator makes resource preparations including scanning tools, targets, steps, determines scan time and methods and give risk alert. Prior to the new system going live, a bug scan must be completed and Information Security Administrator shall prepare and archive an analysis report.

Real-time network packet bug scan – Such scan through the entire system will be carried out with relevant tools and a scan report will be generated on a weekly basis.

Periodic system bug scan - Information Security Administrator shall make an annual IT system bug scan plan and submit it to Information Security Manager for approval.