

Disaster Recovery Manual for FIs and IAPs



Central Bank of Myanmar

1. Introduction, Glossary

VERSION HISTORY

[Provide information on how the development and distribution of the Business Manual was controlled and tracked. Use the table below to provide the version number, the person drafting the revision, the name of the person approving the revised version, the date that particular version was approved, and a brief description of the reason for revising.]

Version	Approved By	Approval Date	Reason
1.0			

Introduction

In the event of a disaster, CBM and related financial institutions need to immediately grasp the damage situation, take necessary recovery measures, and promptly resume operations related to settlement.

To facilitate the restoration process, Disaster Recovery manual describes measures to be taken when CBM-NET data center and related facilities encounter disasters and CBM-NET cannot be operated normally.

This Disaster Recovery manual describes basic information, system operation and business operation for FIs and IAPs to take.

The composition of the Disaster Recovery manual is described below.

Disaster Recovery manual (Basic information for DR operation for FIs and IAPs)

Basic information about disaster situation such as Basic policy in case of disaster, Disasters assumed, Major steps in disaster recovery response, Considerations on database recovery point and Considerations on processing of Multi instruction message.

Disaster Recovery manual (For FIs and IAPs)

This manual contains next 3 topics

- General items: Organizational action and Responses to CBM that FIs and IAPs should take
- System operation: Process required in the system side of FIs and IAPs before using CBM-NET system
- Business operation: Process required to enable FIs/IAPs to resume business using CBM-NET system

For terms used in this manual and not otherwise defined, see “Glossary” in this manual.

1. Glossary

No	Terms	Definition
1	CBS	Core Banking System A back-end system that processes daily banking transactions and posts updates to accounts and other financial records. Core banking systems typically include deposit, loan and credit processing capabilities, with interfaces to general ledger systems and reporting tools. (from Gartner Glossary)
2	CTS	Cheque Truncation System
3	DB	Database
4	DC (data center)	A building, dedicated space within a building, or a group of buildings used to house computer systems and associated components, such as telecommunications and storage systems.
5	DR (Disaster Recovery)	System and/or action to restore computer systems or damaged by natural disasters and man-made disasters
6	DRM (Disaster Recovery Manual)	The manual for Disaster Recovery
7	FI (financial institution)(s)	Commercial banks and state-owned banks other than CBM
8	FI-GW	A gateway system in FIs to connect with CBM-NET to use STP function
9	IAP (Indirect Account Participant)(s)	An entity which can itself establish a direct connection with permissions of both CBM and its Direct Participant to the CBM-NET for the settlement of its own payments through the account of the Direct Participant with CBM.
10	IAP (Indirect Account Participants)	An entity which can itself establish a direct connection with permissions of both CBM and its Direct Participant to the CBM-NET for the settlement of its own payments through the account of the Direct Participant with CBM.

No	Terms	Definition
11	IRD	Internal Revenue Department
12	MPU	Myanmar Payment Union that the institution for Card clearing located at Yangon
13	NPT-DR	Nay Pyi Taw Disaster Recovery site
14	Responsible Staff	CBM-NET user who is registered to execute single-entry transactions, and either to enter or approve double-inspection transactions
15	Staff	CBM-NET user who is registered to execute single-entry transactions and to enter double-inspection transactions
16	STP (Straight Through Processing)	A process which CBM/FIs can send transaction information
17	YGN-CDC	Yangon Container Data Center

Basic information for DR operation

(for FIs and IAPs)

Table of Contents

1. Overview	3
2. Basic policy.....	4
2.1 Prerequisites/Assumptions	4
3. Disasters assumed.....	5
3.1 Disasters assumed in this manual	5
3.2 Disaster situations and countermeasures	5
4. Organizational structure and rolls of CBM-NET System team under CBM Disaster Countermeasures Office.....	9
5. Major steps in disaster recovery response.....	11
5-1 Steps in CBM side	11
5-2 Steps in FIs side	12
6. Details of decision-making process for applying Disaster Recovery manuals	13
6.1 Recognizing of disaster	13
6.2 Activating the CBM Disaster Countermeasures Office	13
6.3 Confirming the severity of disaster	13
6.4 Determining the possibility of business continuity of using YGN-CDC	14
6.5 Making decision to switch to NPT-DR	14
6.6 Making announcement of CBM-NET site switching	15
6.7 Confirming system status of FIs and IAPs participating CBM-NET system	15
6.8 Confirming business operation status of FIs and IAPs participating CBM-NET system	15
7. Considerations on database recovery point	16
8. Considerations on processing of Multi instruction message	18
8-1 Processing mechanism of “Multi instruction message”	18
8-2 Interruption of processing of the “Multi instruction message”	19
8-3 Transaction recovery when interruption of “Multi instruction message” occurred	20
Appendix 1	21
Appendix 2	22
Appendix 3	23
Appendix 4	25

1. Overview

This Manual (DRM Basic) consists of the following sections:

(1) Basic Policy

This section explains basic concept and prerequisites/assumptions for disaster recovery manuals.

(2) Disasters assumed

This section explains the disasters assumed in this manual.

Assuming damage of CBM-NET Container data center, damage of CBM Yangon branch, damage of network between Yangon (YGN hereafter) and Nay Pyi Taw (NPT hereafter), etc.

(3) Organizational structure and rolls of CBM-NET System team under CBM Disaster Countermeasures Office

This section explains the structure and role of CBM-NET System team under CBM Disaster Countermeasures Office in the event of a disaster.

By describing them, the performing and management structure for disaster countermeasures will be clarified and the responsibility will be clarified.

(4) Major processes in disaster recovery response

This section explains the main processes that CBM and CBM-NET participants (Commercial banks and State own banks, IRD, MPU, MFSPs and other participants except CBM, FIs hereafter) should take in the event of a disaster.

FIs also need to understand this process as FIs may be involved.

(5) Decision making process for applying DR manuals

This section explains Decision making process for applying DR manuals.

By clarifying the decision-making process when applying this manual, we aim to provide smooth recovery from disasters.

(6) Considerations on database recovery point

This section explains points to be aware of regarding DB recovery.

(7) Considerations on Multi instruction message processing

This section explains points to be aware of regarding multi instruction message. Processing mechanism of multi instruction message and things what is caused by interruption of process of multi instruction message.

2. Basic policy

- In the event of a disaster affecting an CBM business operations including CBM-NET and CTS system, CBM Disaster Countermeasures Office will work closely with related government agencies and financial institutions.
- Under CBM Disaster Countermeasure Office, CBM-NET System team will take prescribed measures for keeping CBM-NET Continuity in accordance with this manual under the authority given by CBM Disaster Countermeasures Office.
- CBM-NET system places the highest priority on recovering the settlement system in the disaster situations. Therefore, CBM-NET system will be restarted even if some FIs' systems have not been recovered their system.
- CBM-NET system has disaster recovery site in NPT (NPT-DR hereafter). In case of YGN data center is not available by disaster, CBM switches datacenter to NPT-DR.

But NPT-DR is a temporally solution, CBM will switch back to YGN-CDC after completion of recovery of YGN-CDC and YGN office in accordance with the recovery plan of YGN that decided by CBM-NET team and CBM Disaster Countermeasures Office.

In cases where damage of YGN-CDC is so great that hardware and software environment should be newly implemented, it is necessary to consider recovery measures of the YGN data center separately.

2.1 Prerequisites/Assumptions

This disaster recovery manual assumes the following items.

- (1) The disaster recovery manager at CBM is appointed and the Disaster Countermeasures Office is organized in advance. In addition, the personnel responsible for each related department in disaster situations are also appointed in advance. This kind of things will be defined in the Disaster Recovery Plan and Guidelines.
- (2) The personnel who perform works such as confirming the damage status of YGN data center and related facilities in CBM YGN branch must be appointed in advance and be able to work at YGN branch in disaster situations.
- (3) The NPT DR site and CBM headquarters facilities must be available normally when the YGN data center is damaged and cannot be used.
- (4) The system personnel and the manager in charge of the operation of the NPT DR site must be able to come to the NPT head office and can operate the CBM-NET system.
- (5) The personnel who carry out CBM-NET related work and the manager must be able to come to the NPT head office and work, if necessary.
- (6) The minimum means of communication (via mobile phone etc.) between CBM and FIs is available. The emergency contact point list must be made up, maintained up to date and distributed to all necessary organizations including FIs in advance by the disaster countermeasure office.

3. Disasters assumed

3.1 Disasters assumed in this manual

Assuming large-scale earthquakes in the YGN area, fires at the CBM YGN container data center and CBM YGN branch, submerged, and long-term power outages that exceed the continuous power generation period of standby power.

In the case of a large-scale earthquake and long-term power outage in the YGN area, it is expected that the FIs data center and business execution facilities will be damaged.

FIs are expected to make their own Business Continuity Plan for the disaster.

3.2 Disaster situations and countermeasures

- (1) Basic strategy in damage situations and business continuity measures regarding CBM facilities.

The basic strategy is shown in Table 3-1.

Table 3-1: Basic strategy in damage situations of CBM facilities

	YGN-CDC	YGN system operation room	YGN business operation room	Data center and system operation	Business continuity measures
1	Damaged	Usable	Usable	CBM-NET system is switched to NPT-DR. (NPT-DR should be manipulated from NPT operation room only.)	If CBM-NET terminals in YGN office are not usable, the business operations of the YGN branch are taken over at the NPT head office.
2	Damaged	Damaged	Usable		
3	Damaged	Damaged	Damaged		
4	Usable	Damaged	Usable	If YGN-CDC can be manipulated from NPT operation room, the system operation is switched to NPT operation room and use the system in YGN-CDC during business time. After daily batch ended, the system is switched to NPT-DR.	If CBM-NET terminals in YGN office are not usable, the business operations of the YGN branch are taken over at the NPT head office.
5	Usable	Damaged	Damaged	If YGN-CDC cannot be manipulated from NPT operation room, the system is switched to NPT-DR, also.	Business operations of the YGN branch are taken over at the NPT head office.
6	Usable	Usable	Damaged	YGN-CDC is continuously used. (Do not switch data center to NPT-DR)	the business operations of the YGN branch are taken over at the NPT head office.

(2) Assuming damage situations.

Table 3-2-a and Table 3-2-b shows assuming damage situations.

See Table Apdx2-1 (in Appendix 2) for more detail situations about “CBM-NET terminal in FIs”, “FI’s Main-DC” and “FI’s DR-DC”

Table 3-2-a: Disaster situations assumed (Case0 to 5)

CBM-NET Components	Case 0	Case 1	Case 2	Case 3	Case 4	Case 5
YGN-CDC and CBM-NET terminal in CBM	A	A	A	A	A	A
NPT-DR and CBM-NET terminal in CBM	N/A	N/A	N/A	N/A	N/A	N/A
CBM-NET terminal in FIs	A	A	A	D	D	D
FI’s Main-DC	A	D	D	A	D	D
FI’s DR-DC	N/A	A	D or no DR-DC	N/A	A	D or no DR-DC

Legend: A: Available D: Damaged (not available) N/A: Not Applicable

YGN-CDC: CBM YGN Container Data Center

NPT-DR: CBM NPT Disaster Recovery site

DR-DC: Disaster Recovery Data Center (of FI’s)

Table 3-2-b: Disaster situations assumed (Case 6 to 11)

CBM-NET Components	Case 6	Case 7	Case 8	Case 9	Case 10	Case 11
YGN-CDC and CBM-NET terminal in CBM	D	D	D	D	D	D
NPT-DR and CBM-NET terminal in CBM	A	A	A	A	A	A
CBM-NET terminal in FIs	A	A	A	D	D	D
FI’s Main-DC	A	D	D	A	D	D
FI’s DR-DC	N/A	A	D or no DR-DC	N/A	A	D or no DR-DC

Legend: same as Table3-2-a.

(3) Countermeasures according to the damage situations.

Table 3-3 shows countermeasures according to the damage situations defined Table 3-2-a and Table 3-2-b.

Table 3-3: Countermeasures for each Disaster situations assumed

Situations	CBM-NET and FI Status when disaster occurred	Counter measures	Processing method for FIs	
Case0	Normal operation		Web	STP
Case1	CBM-NET and CTS is running. FI cannot use STP due to FI’s Main-DC is not available	FI has their DR-DC and switch to DR-DC. (YGN-CDC and FI’s DR-DC)	Web	STP

Situations	CBM-NET and FI Status when disaster occurred	Counter measures	Processing method for FIs	
Case2(*1)	CBM-NET and CTS is running. FI cannot use STP due to FI's Main-DC is not available.	FI cannot switch to DR-DC because their DR-DC is damaged, or they have no DR-DC. (YGN-CDC and FI's terminal only. FI cannot use STP)	Web	
Case3	CBM-NET and CTS is running. FI cannot use CBM-NET terminal. FI's Main-DC is available.	FI may request CBM to process the business using CBM-NET terminal.	(Web)	STP
Case4	CBM-NET and CTS is running. FI cannot use CBM-NET terminal. FI cannot use STP due to FI's Main-DC is not available.	FI has their DR-DC and switch to DR-DC. (YGN-CDC and FI's DR-DC) FI may request CBM to process the business using CBM-NET terminal.	(Web)	STP
Case5(*1)	CBM-NET and CTS is running. FI cannot use CBM-NET terminal. FI cannot use STP due to FI's Main-DC is not available.	FI cannot switch to DR-DC because their DR-DC is damaged, or they have no DR-DC. FI may request CBM to process the business using CBM-NET terminal.	(Web)	
Case6	CBM-NET and CTS stopped. FI's Main-DC is available.	CBM switches YGN-CDC to NPT-DR. FI re-connect to NPT-DR. (NPT-DR and FI's Main-DC)	Web	STP
Case7	CBM-NET and CTS stopped. FI's DR-DC is available.	CBM switches YGN-CDC to NPT-DR. FI has their DR-DC and switch to DR-DC (NPT-DR and FI's DR-DC)	Web	STP
Case8(*1)	CBM-NET and CTS stopped.	CBM switches YGN-CDC to NPT-DR. FI cannot switch to DR-DC because their DR-DC is damaged, or they have no DR-DC.	Web	

Situations	CBM-NET and FI Status when disaster occurred	Counter measures	Processing method for FIs	
		(NPT-DR and FI's terminal only. FI cannot use STP)		
Case9	CBM-NET and CTS stopped. FI cannot use CBM-NET terminal. FI's Main-DC is available.	CBM switches YGN-CDC to NPT-DR. FI may request CBM to process the business using CBM-NET terminal. (NPT-DR and FI's Main-DC)	(Web)	STP
Case10	CBM-NET and CTS stopped. FI cannot use CBM-NET terminal. FI's DR-DC is available.	CBM switches YGN-CDC to NPT-DR. FI has their DR-DC and switch to DR-DC. FI may request CBM to process the business using CBM-NET terminal. (NPT-DR and FI's DR-DC)	(Web)	STP
Case11(*1)	CBM-NET and CTS stopped. FI cannot use CBM-NET terminal.	CBM switches YGN-CDC to NPT-DR. FI cannot switch to DR-DC because their DR-DC is damaged, or they have no DR-DC. FI may request CBM to process the business using CBM-NET terminal.	(Web)	

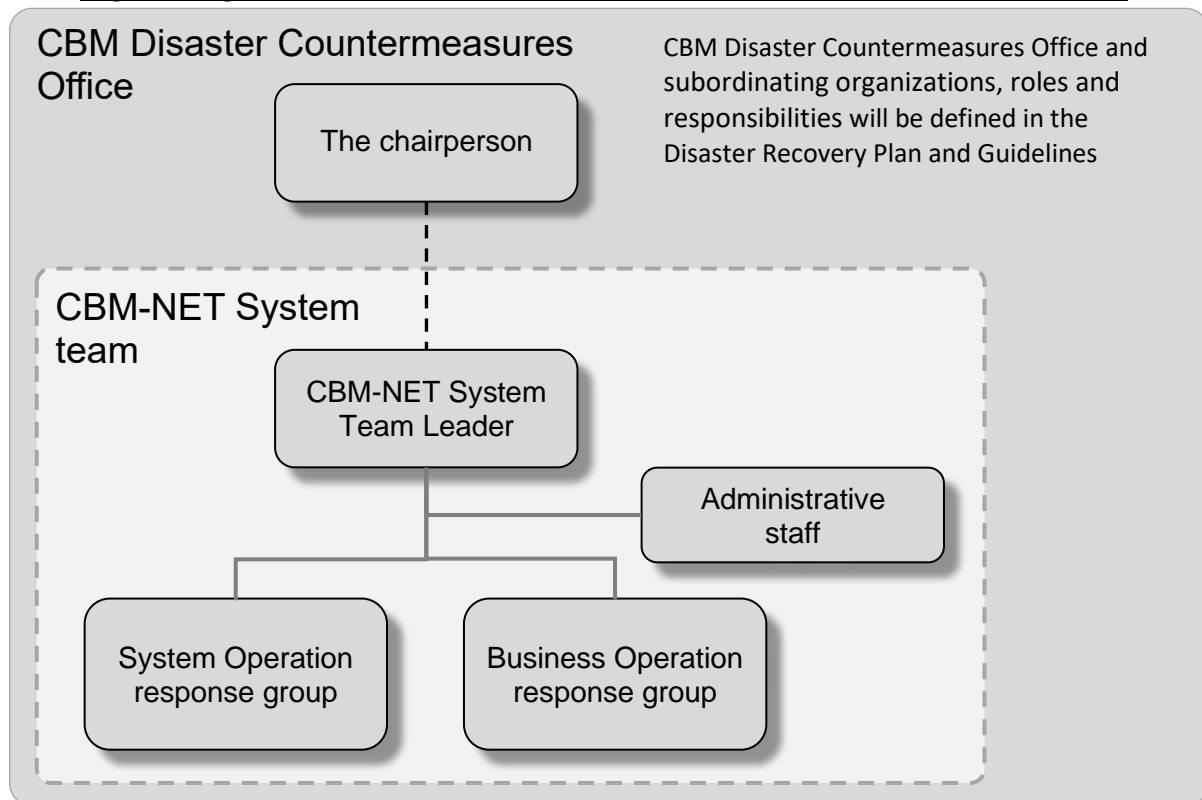
*1: In case of some FIs are in these cases, CBM-NET will restart with cutting them off.

4. Organizational structure and rolls of CBM-NET System team under CBM Disaster Countermeasures Office

CBM Disaster Countermeasures Office and subordinating organizations, roles and responsibilities will be defined in the Disaster Recovery Plan and Guidelines.

In this section, organizational structure and roles of the team which is responsible for disaster countermeasure of CBM-NET System is described.

Fig4-1: Organizational structure of Disaster Countermeasures Office in CBM



(1) CBM-NET System team (part of CBM Disaster countermeasures Office)

- This team manages all relevant information about CBM-NET disaster recovery response and responsible for all decision makings about CBM-NET disaster recovery response, both system operation and business operation relating CBM-NET.
- This team will also give the direction to departments in CBM if necessary.
- Director General of Accounting Department will in charge of the leader of the team.

(2) System Operation response group

- System Operation response group will be in charge of continuity management of CBM-NET system as a IT system.

This group will be responsible to following items and take recovery actions according to the Disaster Recovery manual (System operation).

- a. Data center switching
- b. Database recovery
- c. Network reconnection and other necessary recovery actions

- d. Communication with FIs and CBM internal departments
- Director of AHRD, who is in charge of IT system management will be in charge of the group leader and has the necessary authority to proceed with disaster recovery response of CBM-NET system.

(3) Business Operation response group

- Business Operation response group will be in charge of continuity management of business running on CBM-NET and CTS system and take necessary business recovery actions.
- This group will take recovery actions for business operation as follows.
 - a. Determination of the restart point from the business continuity perspective
 - b. Providing necessary instructions or directions to FIs
 - c. Decisioning about operating time of the CBM-NET and CTS systems, such as operating time extension and shortening and also not restarting
 - d. Communication with FIs and CBM internal departments
- Deputy Director General of PSSD, who is in charge of CBM-NET related business, will be in charge of the group leader and has the necessary authority to proceed with recovery response for CBM-NET and CTS system related business.

(4) Administrative staff

- Administrative staff will assist the leader of CBM-NET System team, and will be responsible for various administrative tasks such as preparing the conference rooms and remote conference facilities, creating reports and organizing information.
- Administrative staff will maintain series of “Disaster Recovery manual” including emergency contact point list and distribute them to necessary organizations.
- Director of PSSD / AHRD will be assigned as an Administrative staff.

(5) Abbreviations for CBM-NET System team

SOG-Y: System Operation response group in Yangon
 SOG-N: System Operation response group in Nay Pyi Taw
 BOG-Y: Business Operation Group in Yangon
 BOG-N: Business Operation Group in Nay Pyi Taw
 AdmS-S: Administrative staff of system operation
 AdmS-B: Administrative staff of business operation

5. Major steps in disaster recovery response

When disaster occurred, CBM and FIs have to take actions to keep continuity of business and minimize the adverse effects of disasters.

The major steps that CBM and FIs should take in the event of a disaster are as follows:

(See “Fig Apdx3-1: Chart of Process step relations in disaster recover response” which describes relation between each steps)

5-1 Steps in CBM side

The steps that CBM should take in the event of a disaster is as follows:

Step-1. Decision making for switching to NPT-DR

This step is almost same the steps of decision-making process for applying Disaster Recovery manual. Details are written in DRM “Basic” (this manual).

(This step will be done by CBM-NET System team led by CBM-NET System Team Leader with cooperation of SOG, BOG and AdmS)

1-0. Disaster occurrence

1-1. Recognizing of disaster

1-2. Activating CBM Disaster Countermeasures Office

CBM Disaster Countermeasures Office and CBM-NET System team will be activated.

1-3. Confirming the severity of disaster

Health check of CBM-NET, YGN-CDC, NPT-DR, etc.

For details, refer to DRM “System operation for CBM”.

1-4. Determining whether business can be continued using YGN-CDC

1-5. Making decision to switch to NPT-DR

1-6. Announcement of CBM-NET site switching (YGN-CDC to NPT-DR)

1-7. Confirming system status of FIs and IAPs participating CBM-NET system (SOG and AdmS-S)

1-8. Confirming business operation status of FIs and IAPs participating CBM-NET system (BOG and AdmS-B)

Step-2. System operation for site switching

Details are written in DRM “System operation for CBM”.

(This step will be done by SOG.)

2-1. Confirming database availability on NPT-DR site

2-2. Turn over to NPT-DR and make announcement to FIs of completion of site change

2-3. Connection with FIs

2-4. Confirming the completion of turn over to NPT-DR

2-5. Release to application

Step-3. Business operation for restart using NPT-DR

Details are written in DRM “Business operation for CBM”

(This step will be done by BOG.)

3-1. Confirming overall progress of daily operations of the CBM-NET

3-1-1. Confirming progress status

3-1-2. Make CBM-NET operation schedule for the day and thereafter and make announcement

3-2. CBM-NET terminal connection

3-2-1. Confirming restart point

3-2-2. Recovery and resuming business using CBM-NET terminal (Both for CBM itself and based on application from FIs)

- 3-3. STP connection
 - 3-3-1. Confirming restart point
 - 3-3-2. Inform latest transaction completed in CBM-NET to FIs
- 3-4. File Uploaded Transaction
 - 3-4-1. Confirming restart point
 - 3-4-2. Recovery and resuming business using File upload (Both for CBM itself and based on application from FIs)
- 3-5. CTS
 - 3-5-1. Confirming restart point
 - 3-5-2. Recovery and resuming business of CTS
- 3-6. Support for FIs and IAPs using NPT-DR
 - 3-6-1. Confirming the situation of all FIs and IAPs participating CBM-NET system
 - 3-6-2. Providing information of CBM-NET system operation using NPT-DR
 - 3-6-3. Support for FIs and IAPs for business operation using NPT-DR

5-2 Steps in FIs side

The major steps that FIs should take in the event of a disaster are as follows:

Step-1. Initial actions to be taken as disaster response for CBM-NET and FI's main IT system (mainly Core Banking System)

This step is almost same as step for CBM, and details should be decided in each FIs/IAPs.

- 1-0. Disaster occurrence
- 1-1. Recognizing of disaster
- 1-2. Activating the disaster response organization
- 1-3. Confirming the severity of disaster

Step-2. System recovery

Details are written in DRM "System operation for FIs and IAPs".

- 2-1. Damage determination and confirmation
- 2-2. Site change of FI's main IT system to FI's DR site and recover database if needed
- 2-3. Connection change to NPT-DR after completion of CBM's site switching
- 2-4. Connection change confirmation and informing to CBM

Step-3. Business operation

Details are written in DRM "Business operation for FIs and IAPs".

- 3-1. CBM-NET terminal connection
 - 3-1-1. Confirming restart point
 - 3-1-2. Recovery and resuming business using CBM-NET terminal.
- 3-2. STP connection
 - 3-2-1. Inquire to and receive from CBM-NET of completed messages (upstream and downstream) by CBM-NET
 - 3-2-2. Confirming restart point
 - 3-2-3. Recovery and resuming business using STP
- 3-3. File Uploaded Transaction
 - 3-3-1. Confirming restart point
 - 3-3-2. Recovery and resuming business using File upload
- 3-4 CTS
 - 3-4-1. Confirming restart point
 - 3-4-2. Recovery and resuming business of CTS

6. Details of decision-making process for applying Disaster Recovery manuals

The steps for deciding to apply this disaster recovery manual in the event of a disaster is a part of “Decision making for switching to NPT-DR”.

The steps are as follows:

0. Disaster occurrence
1. Recognizing of disaster
2. Activating CBM Disaster Countermeasures Office
3. Confirming the severity of disaster
4. Confirming the NPT-DR availability
5. Determining whether business can be continued using YGN-CDC
6. Making decision to switch to disaster recovery site (NPT-DR)
7. Confirming system status of FIs and IAPs participating CBM-NET system
8. Confirming business operation status of FIs and IAPs participating CBM-NET system

After that, according to the manual, proceed to work for switching data center and for resuming business.

6.1 Recognizing of disaster

When a disaster occurs, the countermeasure process begins by recognizing the situations.

CBM will recognize the occurrence of a disaster and the system failure caused by the disaster by followings

1. Large-scale of earthquakes, flooding, fires, etc. that may impact on the data center will be recognized through local communications, news reports, etc.
2. Notification of system failure
Recognize system failure by receiving information of failure from data center operators, CBM staff, and FI's staff, who detected system faults.
(It is necessary to assign a contact person in charge and make it known to related organizations.)

6.2 Activating the CBM Disaster Countermeasures Office

After recognizing the occurrence of a disaster, CBM must activate CBM Disaster Countermeasures Office and CBM Disaster Countermeasures Office must activate CBM-NET System Team to proceed with actions according to the disaster situations.

CBM-NET System Team must be organized in advance.

CBM-NET System Team has the necessary authority to proceed with disaster countermeasures for CBM-NET system.

6.3 Confirming the severity of disaster

It is necessary to confirm the severity of the disaster in order to take necessary measures according to the disaster situations.

The following are the possible confirmation items for the disaster situations:

- Status of CBM-NET (by SOG-Y)
- Status of YGN-CDC (including power supply status) (by SOG-Y)
- Status of NPT-DR (including power supply status) (by SOG-N)

- Status of network environment related to CBM-NET (by SOG-Y and SOG-N)
- Status of CBM-YGN branch building (including power supply status) (by SOG-Y and/or BOG-Y)
- Status of CBM-NPT head office building (including power supply status) (by SOG-N and/or BOG-N)
- Status of the means of communication with CBM related departments (by AdmS-S and AdmS-B)
- Status of FI's disaster response organization and emergency contact point, their main datacenter, DR datacenter and business operation office, etc. (by AdmS-S and AdmS-B)

For detail procedure of checking and confirming disaster situations of CBM-NET system, CTS system and related network, please refer to “DRM System operation for CBM”.

6.4 Determining the possibility of business continuity of using YGN-CDC

Based on the information collected and confirmed in previous step, consider whether it is possible to continue CBM-NET operations using YGN-CDC or should switch to NPT-DR.

This will be done by SOG and BOG.

The following may be the considerations for judgment.

- (1) Availability of continued use of YGN-CDC itself (by SOG-Y)
 - If there is a failure on the devices that make up CBM-NET or not.
 - If there is a failure, the time required for recovery, or if it is possible or not to disconnect and operate the device which has failure.
 - Influence of CBM-NET operation when the container is physically damaged
 - In case that the physical damage makes an impact on CBM-NET operation, how long will it require for recovery.
 - Securing power supply (If power is in lost situations, standby power generation continuation time is enough or not)
- (2) Network between YGN-CDC and commercial banks be usable without problems or not. (by SOG-Y and SOG-N)
- (3) NPT-DR is useable normally and can be switched. (by SOG-N)
- (4) Time required for switching to NPT-DR. (by SOG-N and SOG-Y)
 - Time required for system switchover (CBM-NET system starting time and connection change with FIs) .
 - Performing and confirming of business recovery on both CBM side and FIs' side (especially confirmation of incomplete transactions in progress) .

If it is possible to recover YGN-CDC in a short period of time, it may be safer to wait for the recovery than to switch to NPT-DR.

6.5 Making decision to switch to NPT-DR

Considering these, decide to switch to NPT-DR in case that switching to NPT-DR is a better strategy.

CBM-NET System Team Leader will make this decision.

Once the decision to switch to NPT-DR is made, the related teams will follow the DR manuals to proceed to work for switching data center and subsequent business operations for resuming business.

6.6 Making announcement of CBM-NET site switching

When CBM decided to switch YGN-CDC to NPT-DR, CBM will announce data center switch to CBM-NET participating FIs and IAPs.

This will be done by AdmS-S, because FIs and IAPs must do connection change to NPT-DR.

6.7 Confirming system status of FIs and IAPs participating CBM-NET system

After CBM-NET System Team is activated, CBM should check the system status of FIs and IAPs participating CBM-NET system to get an overall picture.

This will be done by AdmS-S.

6.8 Confirming business operation status of FIs and IAPs participating CBM-NET system

After CBM-NET System Team is activated, CBM should check the business operation status of FIs and IAPs participating CBM-NET system to get an overall picture.

This will be done by AdmS-B.

For summarizing the status of all participating FIs' system and business operation status, it is preferable that CBM makes the list of the status confirmed.

Fig 6-1 shows an example of the list.

Fig6-1: System and business operation status list

			CBM-NET System						CTS		
			CBM-NET terminal		STP		File Upload				
NO.	Participants	CBS	Own	Alt	Own	Alt	Own	Alt	Own	Alt	Remarks
1	A Bank	OK (Primary)	OK		OK(Full)		OK		OK		
2	B Bank	OK (DR)	OK		OK(Partial)		OK		OK		
3	C Bank	NG (no DR)	NG	CBM-NPT	NG	X Bank	NG	CBM-NPT	NG	X Bank	
...	...										
...	...										

Own: Own site

Alt: Alternative method

7. Considerations on database recovery point

There is an important consideration points on database recovery point of CBM-NET system.

there are 3 main database owner systems in CBM-NET system, sender FI's system, CBM-NET system and receiver FI's system.

When disaster occurred, these 3 database owner systems may should recover each database.

Because of the database replication and recovery specification for disaster recovery of the CBM-NET system, the results of some transactions performed at the YGN-CDC before the disaster may be lost from the database of the CBM-NET system restarted at the NPT-DR.

The CBM-NET is constituted by CBM-NET system on CBM site, sender-FI system and receiver-FI system, and they are processing asynchronously.

Therefore, in a system restart time points after the disaster, inconsistencies may occur in the progress results of transactions recognized by the three parties, CBM-NET system, sender-FI system, and receiver-FI system.

Explain using sample time flow of: T0 ---> T1 ---> T2 ---> T3---> T-D

T0: system starting point of a day

T1: some point of time after T0

T2: some point of time after T1

T3: some point of time after T2

T-D: time point disaster occurred

In this time flow, suppose that processing has been completed up to T3, and then a disaster occurred.

Systems its database was affected by the disaster have to recover them. And database recovery point of each system may be different.

The CBM-NET system will adopt the database recovered at NPT-DR as a restart point (Reference point hereafter), even if some transactions were lost.

FIs must use this reference point as the base point for resuming processing.

Database here means database of CBM-NET application, not the database of CBM-NET Gateway. Transactions, received by CBM-NET Gateway and not sent to CBM-NET application at the disaster strike, will not be recovered when CBM-NET system restarted.

The following combinations of recovery points for these 3 systems are possible.

Table7-1: Database Recovery point combinations and Action to be taken

	Sender FI	CBM-NET	Receiver FI	Action to be taken
Case1	T3	T3	T3	Reference point is T3. All three components recovered to the same point after the recovery process. Resume processing from the transaction following the last transaction completed just before the disaster occurred

	Sender FI	CBM-NET	Receiver FI	Action to be taken
Case2	T3	T3	T2	Reference point is T3. Receiver FI needs to catch up to T3 before another FIs resume processing.
Case3	T2	T3	T3	Reference point is T3. Sender FI needs to catch up to T3 before another FIs resume processing.
Case4	T2(*1)	T3	T2(*1)	Reference point is T3. Both Sender FI and receiver FI needs to catch up to T3 before another FIs resume processing.
Case5	T3(*1)	T2	T3(*1)	Reference point is T2. Both Sender FI and receiver FI needs to cancel or reverse the transaction processed between T2 and T3 to return to T2.
Case6	T3	T2	T2	Reference point is T2. Sender FI needs to cancel or reverse the transaction processed between T2 and T3 to return to T2.
Case7	T3	T2	T1	Reference point is T2. Sender FI needs to cancel or reverse the transaction processed between T2 and T3 to return to T2. Receiver FI needs to catch up to T2 before another FIs resume processing.
Case8	T2	T2	T3	Similarly, FIs that are ahead of the CBM's recovery point need to return to CBM's recovery point, and those that are behind need to catch up to CBM's recovery point.
Case9	T1	T2	T3	
Case10	T2	T2	T2	
Case11	T2	T1	T3	
Case12	T3	T1	T2	

*1 Note: Understand that Sender Fi T2/T3 and Receiver FI T2/T3 do not necessarily mean the exact same timing, but that they are behind/ahead of the CBM recovery point T3/T2.

8. Considerations on processing of Multi instruction message

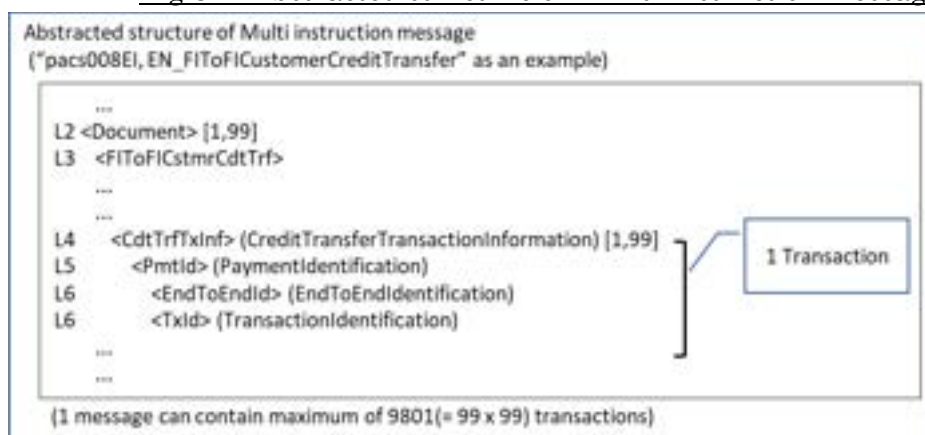
In this manual, a message that contains multiple instructions are called "Multi instruction message".

Understanding the processing mechanism of Multi instruction message will be helpful to understand things what is caused by interruption of processing of Multi instruction message.

8-1 Processing mechanism of "Multi instruction message"

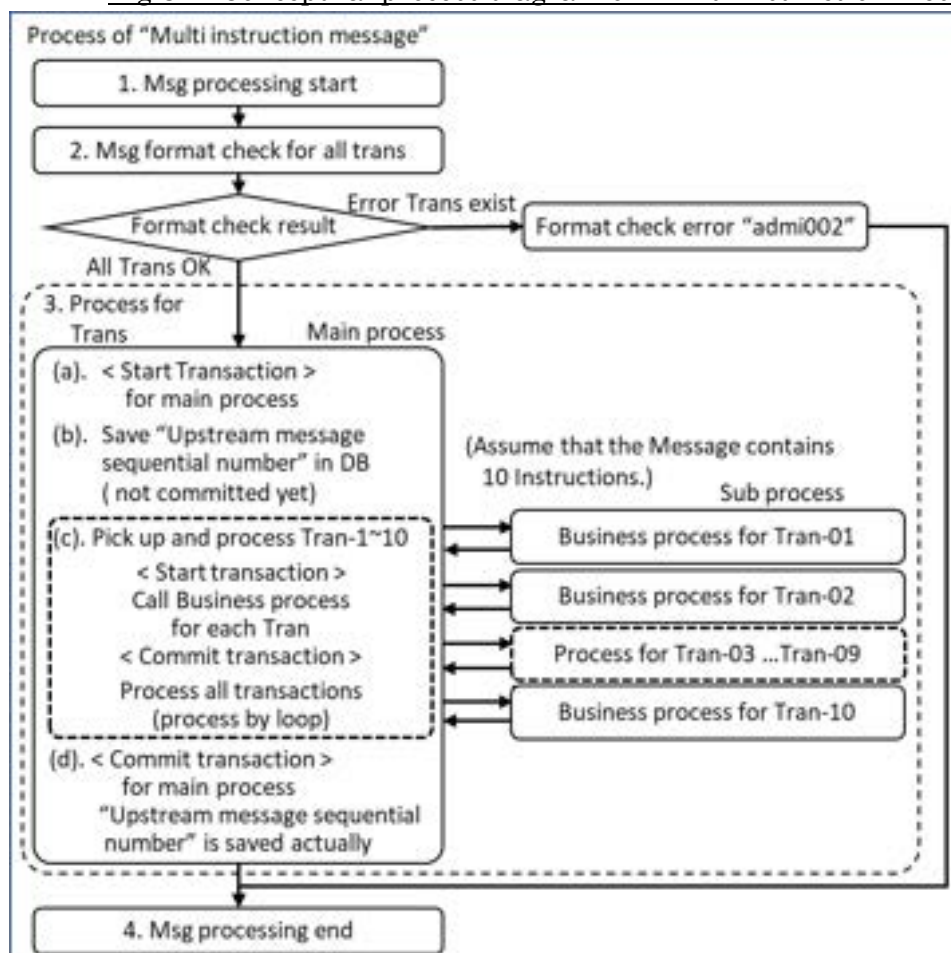
Abstracted structure of "Multi instruction message" is as follows.

Fig 8-1: Abstracted structure of "Multi instruction message"



Processing mechanism of "Multi instruction message" is shown if Fig 8-2.

Fig 8-2: Conceptual process diagram of "Multi instruction message"



In this example, 10 transactions (instructions) will be processed in 1 message processing.

Main process starts transaction before it calls sub process and commits transaction after returned from sub process. Sub process is a business process which processes 1 transaction when it is called by main process.

This means transaction will be completed sequentially.

Business check will be done in sub process.

In case of without business check error, acceptance and/or instruction notification is notified in Single message. (pacs002/pacs008)

In case of business check error, error message is notified in Single message as same as acceptance notification.

The process of the “Multi instruction message” will complete when processing of all transactions (instructions) contained in the message finished and also “Upstream message sequential number” will be saved in database actually at this point.

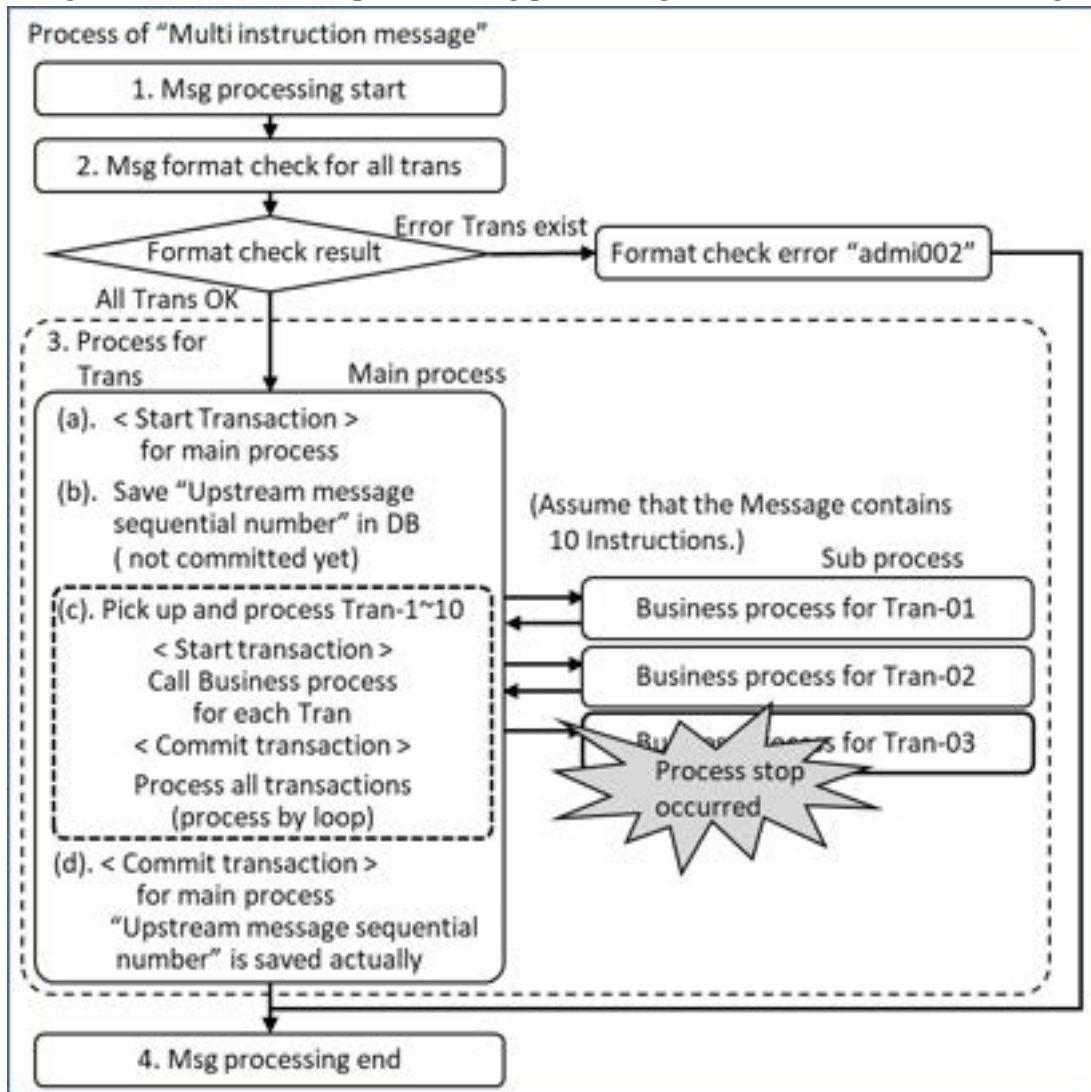
8-2 Interruption of processing of the “Multi instruction message”

When interruption of processing of the “Multi instruction message” occurred, the transactions (instructions) committed before interruption have been completed, whether process result was a normal or an error.

Fig 8-3 shows the case of interruption occurred during processing the “Multi instruction message”. In this case, interruption occurred in the middle of processing Tran-03. Tran-01 to Tran-02 are completed and Tran-03 to Tran-10 are not completed.

When this case happened, Tran-03 to Tran-10 must be sent to CBM-NET again to process them.

Fig 8-3: Process interruption during processing of “Multi instruction message”



8-3 Transaction recovery when interruption of “Multi instruction message” occurred

When interruption of “Multi instruction message” occurred, “Upstream message sequential number” of this message will not be saved actually in database. This means that this “Multi instruction message” will be treated as a lost message for CBM-NET application when FIs request to get information of message counter and message sequential number to CBM-NET using

“STP010 STP counter notification (STP010_admi009EI StaticDataRequest)”.

According to this information, FIs will resend this “Multi instruction message”.

When FIs resend this “Multi instruction message”, CBM-NET returns error notification of “Transaction Identification duplicate error” for Tran-01 and Tran-02 because they were already processed before disaster occurred. Tran-03 to Tran-10 will be processed as a new transaction (instructions).

FIs should ignore this “Transaction Identification duplicate error” message in the disaster recovery situations.

Appendix 1

Emergency contact point list (in disaster situations)

Organization	Department	Contact person (Name)	Phone no.	Mail address
CBM				
XX bank				

Appendix 2

Table Apdx2-1: Disaster situations assumed details for FI's Data Center and CBM-Net terminal

CBM-NET Components	Case M1	Case M2	Case M3	Case M4	Case M5	Case M6	Case D1	Case D2	Case D3	Case D4	Case D5	Case D6
YGN-CDC and CBM-NET terminal in CBM	A	A	A	D	D	D	A	A	A	D	D	D
NPT-DR and CBM-NET terminal in CBM	N/A	N/A	N/A	A	A	A	N/A	N/A	N/A	A	A	A
FI's Main-DC	A	D	D	A	D	D						
FI-Main-DC (with FI-GW for FI-Main-DC)	A	D	A	A	D	A						
N/W YGN-CDC and FI Main-DC	A	N/A	D	N/A	N/A	N/A						
N/W NPT-DR and FI Main-DC	N/A	N/A	N/A	A	N/A	D						
FI's DR-DC							A	D	D	A	D	D
FI-DR-DC (with FI-GW for FI-DR-DC)							A	D	A	A	D	A
N/W YGN-CDC and FI-DR-DC							A	N/A	D	N/A	N/A	N/A
N/W NPT-DR and FI-DR-DC							N/A	N/A	N/A	A	N/A	D

	Case CDC1(*1)	Case CDC2(*1)	Case DR1(*2)	Case DR2(*2)
CBM-NET terminal in FIs	A	D	A	D
N/W YGN-CDC and FI(CBM Terminal)	A	D	N/A	N/A
N/W NPT-DR and FI(CBM Terminal)	N/A	N/A	A	D

Legend: A: Available D: Damaged (not available) N/A: Not Applicable

YGN-CDC: CBM YGN Container Data Center

NPT-DR: CBM NPT Disaster Recovery site

DR-DC: Disaster Recovery Data Center (of FI's)

(*1): Case of YGN-CDC running

(*2): Case of NPT-DR running

Appendix 3

Fig Apdx3-1 Chart of process step relations in disaster recover response (1/2)

work category	work name	sub work	CBM				Fis and IAPs			
			Action	reference steps	information gathering	reference steps	Action	reference steps		
pre work	preparation for disaster response	develop BCP and/or disaster recovery plan	BCP and/or disaster recovery plan development				BCP and/or disaster recovery plan development			
		organize disaster response organization	organizing disaster countermeasures office including CBM-NET System team and assign responsible persons				organizing disaster response organization and assign responsible persons			
		maintain contact point list	maintain contact point list of CBM and Fis gather Fis' contact point list at the point of annual disaster response drill		Make/maintain contact point list of CBM and CBM-NET participants	prearranges	maintain contact point list of Fis and report it to CBM at least once a year			
Before CBM-NET site switch	decision making for switching to DR-site	Activating disaster response organization	Activating CBM Disaster Countermeasure Office	Step 1-2			Activating the disaster response organization	Step 1-2		
		Confirming the severity of disaster	Conduct Health check	Step 1-3			Confirming the severity of disaster	Step 1-3		
			(as a part of Health check, CBM broadcasts disaster recognition and requesting status report to Fis and IAPs)		Confirm status of Fis disaster response organization and emergency contact point, their main datacenter, DR datacenter and business operation office, etc.	Step 1-3	Issue status report via Inter bank message as a respond to broadcast message from CBM			
			check business continuing availability using NGN-CDC		Step 1-4					
		Decision making of datacenter switching	decision making to switch to NPT-DR	Step 1-5			Decision making to switch to Fis DR-site if necessary			
		Announcement of datacenter switch	Announce to Fis of CBM-NET site switching (NGN-CDC to NPT-DR)	Step 1-6						
	★Check point 1	Confirm all CBM-NET participants recognize CBM-NET site switching			Make confirmation summary		Inform to CBM the CBM-NET site switching recognition in response to CBM inquiry		Step 2-2	
	CBM-NET site switching	Site switching	Turn over to NPT-DR	Step 2-1	Confirming system status of Fis and IAPs participating CBM-NET system	Step2-7	Switch to Fis DR-site if necessary before connection change to NPT-DR			
			Make announcement to Fis of CBM-NET site switch completion	Step 2-2						
		Re-connection to DR-site	Connection with Fis	Step 2-3	Confirming business operation status of Fis and IAPs participating CBM-NET system	Step2-8	Connection change to NPT-DR	Step 2-3		
			Confirming the completion of turn over to NPT-DR	Step 2-4			Connection change confirmation and informing to CBM	Step 2-4		
	★Check point 2	Confirm all CBM-NET participants reconnected to NPT-DR			Make confirmation summary		Inform to CBM the connection status in response to CBM inquiry			
	Preparation for resuming business	Confirming overall progress of daily operations of the CBM-NET	Confirming overall progress of daily operations of the CBM-NET	Step 3-1-1						
			Confirming restart point of CTS	Step 3-3-1						
			Make CBM-NET operation schedule for the day and thereafter	Step 3-1-2						
		preparation of resuming CTS	Recovery and resuming business of CTS	Step 3-3-2						

Fig Apdx3-1 Chart of process step relations in disaster recover response (2/2)

work category	work name	sub work	CBM				FIs and IAPs	
			Action	reference steps	information gathering	reference steps	Action	reference steps
Business operation after CBM-NET site switch	★Check point 3	1. Announce to FIs to get information before restart business instruction process using CBM-NET on NFT-DR and confirm all participants completed getting information. Information to get is a. Each FI branch's balance of current account, LSP account b. Each FI's balance of collateral amount, debit cap, debit allowance c. Each FI branch's balance of USD account and other currency account if using d. Each FI's balance of T-bond/bill proprietary account, customer account, pledged account e. Upstream message : message counter, message sequential number (From/To), Sequential number part of Non-existing Upstream message sequential number list f. Downstream message : message counter, message sequential number (From/To)			Step 3-3-2	Make confirmation summary	Inform to CBM that FI get information about balance, statement and Upstream/Downstream message sequential number and counter a. balance of current account, LSP account : FBS10_FundBalanceInquiry b. balance of collateral amount : CBS10_CollateralBalanceInquiry balance of debit cap, debit allowance : DCS10_DebitCapInquiry c. balance of USD account and other currency account if using : FBS10_FundBalanceInquiry (USD, EUR, SGD, JPY) d. balance of T-bond/bill proprietary account, customer account, pledged account : FBS10_BondBillBalanceInquiry e. f. Upstream/Downstream message sequential number and counter : STP010 STP counter notification (STP010_admin008E StaticDataRequest)	
	★Check point 4	1. Announce to FIs of restart of CBM-NET using NFT-DR, and restart business operation and necessary recovery in its 2. Instruct participant banks the action to take for recovery of CTS system			Step 3-3-2	Make confirmation summary	Inform to CBM the CBM-NET restart using NFT-DR and action for CTS in response to CBM inquiry	
	Confirming restart point	for CBM-NET terminal	Confirming restart point of business using CBM-NET terminal	Step 3-3-1			Confirming restart point of business using CBM-NET terminal	Step 3-3-1
		for STP	Confirming restart point of business using STP (no CBM action needed)	Step 3-3-1 Step 3-3-2			Confirming restart point of business using STP	Step 3-3-1 Step 3-3-2
		for File upload	Confirming restart point of business using File upload	Step 3-4-1			Confirming restart point of business using File upload	Step 3-3-1
		for CTS					Confirming restart point of CTS	Step 3-4-1
	Recovery and resuming business	for CBM-NET terminal	Recovery and resuming business using CBM-NET terminal	Step 3-3-2			Recovery and resuming business using CBM-NET terminal	Step 3-3-2
		for STP					Recovery and resuming business using STP	Step 3-3-3
		for File upload	Recovery and resuming business using File upload	Step 3-4-2			Recovery and resuming business using File upload	Step 3-3-2
		for CTS					Recovery and resuming business of CTS	Step 3-4-2
	★Check point 5	Confirming the status of CBM-NET system using NFT-DR and business operation			Step 3-5-1	Confirming system status and business operation status of FIs and IAPs participating CBM-NET system Make confirmation summary	Inform to CBM the system and business operation status	

Appendix 4

Fig Apdx4 Sample of Status summary List at Disaster recognition

[illegible]

General items for DR operation for FIs and IAPs

Table of Contents

1. Overview	3
2. Organizational action FIs and IAPs should take	4
2.1 Actions of preparation for disaster	4
2.2 Actions to respond to the disaster	4
3. Responses to CBM	5
3.1 Responses to CBM, as a preparation for disaster response and as a disaster response actions in disaster situation.....	5

1. Overview

This Manual (DRM General items for FIs and IAPs) explains actions should be done by FIs and IAPs in disaster situations in the sections as follows.

(1) Organizational action FIs and IAPs should take

This section explains the organizational actions that FIs and IAPs should take to respond to disaster.

It contains organizational preparations for disaster and actions in disaster situation.

(2) Responses to CBM

This section explains the necessary responses to CBM in disaster situation.

2. Organizational action FIs and IAPs should take

In this section, organizational actions needed as a preparation for disaster and response to the disaster when it occurred are described.

FIs and IAPs should follow the Guidelines which CBM will provide.

2.1 Actions of preparation for disaster

FIs and IAPs should make preparation for the disaster as follows.

- Develop business continuity plan, disaster recovery plan and disaster recovery manual to secure business continuity in disaster situations.
- Build up the disaster response organization for taking quick and appropriate actions in disaster situations.
- Make emergency contact point list of the disaster response organization and contact person and provide them to CBM. It should be maintained and provided to CBM when organization and contact person change occurred.
- It would be considered to secure the way of CBM-NET related business and CTS business in the situation of all channel to CBM-NET system and CTS system was damaged and FIs and IAPs cannot continue business using their own site and facilities when disaster occurred. Outsourcing the work to another FI is one of the possible methods.

2.2 Actions to respond to the disaster

FIs and IAPs should take disaster response actions according to the disaster recovery manual when disaster occurred.

In a disaster situation, it is important to act in concert with the entire organization and the CBM and other FIs.

2.2.1 Steps to be taken when disaster occurred.

Followings are the major steps that FIs should take in the event of a disaster.

It is important that these steps be reviewed and documented in the Disaster Recovery/ Response Manual of FIs' own.

Step-1. Initial actions to be taken as disaster response for CBM-NET and FI's main IT system (mainly Core Banking System)

This step is almost same as step for CBM, and details should be decided in each FIs/IAPs.

- 1-0. Disaster occurrence
- 1-1. Recognizing of disaster
- 1-2. Activating the disaster response organization
- 1-3. Confirming the severity of disaster

Step-2. System recovery

Details are written in DRM "System operation for FIs and IAPs".

- 2-1. Damage determination and confirmation
- 2-2. Site change of FI's main IT system to FI's DR site and recover database if needed
- 2-3. Connection change to NPT-DR if CBM's site switching occurred
- 2-4. Connection change confirmation and informing to CBM

Step-3. Business operation

Details are written in DRM “Business operation for FIs and IAPs”.

- 3-1. CBM-NET terminal connection
 - 3-1-1. Confirming restart point
 - 3-1-2. Making preparation of resuming business using CBM-NET terminal.
- 3-2. STP connection
 - 3-2-1. Inquire to and receive from CBM-NET of completed messages (upstream and downstream) by CBM-NET
 - 3-2-2. Confirming restart point
 - 3-2-3. Making preparation of resuming business using STP
- 3-3. File Uploaded Transaction
 - 3-3-1. Confirming restart point
 - 3-3-2. Making preparation of resuming business using File upload
- 3-4. CTS
 - 3-4-1. Confirming restart point
 - 3-4-2. Making preparation of resuming business of CTS
- 3-5 Resume Business operation using NPT-DR
 - 3-5-1. Informing CBM of completion of preparation to resume business using STP, File upload and CTS
 - 3-5-2. Receiving announcement of resume Business operation using NPT-DR by CBM
 - 3-5-3. Resume business operation using CBM-NET terminal, STP, File upload and CTS

3. Responses to CBM

FIs and IAPs should follow the Guidelines and specific instructions which CBM will provide.

But basically, FIs and IAPs should take actions as a preparation for disaster response and as a disaster response actions in disaster situation and inform/report next items to CBM.

< Preparation >

- Disaster response organization and contact point list
Structure of the disaster response organization and emergency contact point list at least 1 time per year and when they are changed.

< Disaster response action >

- Status of the disaster response organization
Activating status of the disaster response organization and action plans when disaster occurred.
- Severity of disaster and actions to take
Result and/or situation about next points.
 - Damages on office, Data center (Main center, DR site)
 - Need or not need to switch data center to DR site
 - System operating status (CBS, internal CTS, CBM-NET (STP and CBM-NET terminal, CTS)
 - Impact on business
 - Estimated recovery time
- Completion of connection change to NPT-DR if CBM’s site switching occurred
- Completion of preparation of resuming business

CBM-NET terminal, STP, File Upload, CTS

- Result of recovery action and situation of system and business operations
- Other items required by CBM

System operation for FIs and IAPs

Table of Contents

1. Overview	3
2. Damage determination and confirmation.....	4
2.1 Confirmation of the availability of CBM-NET terminals	4
2.2 Confirmation of the availability of CBS and FI-GW	5
2.3 Confirmation of the availability of network connection to CBM-NET	5
3. Confirmation of the operation site of CBS.....	7
4. Connection change to NPT-DR.....	8
5. Connection change confirmation and informing to CBM	8
Appendix-1	エラー! ブックマークが定義されていません。

1. Overview

When a disaster occurs and YGN-CDC for CBM-NET cannot be used, the CBM-NET system will be switched to the NPT-DR site and the database will be restored by system operations.

The user of CBM-NET systems, such as FIs and IAPs, also have to confirm the status of own environment and prepare for restarting the business using CBM-NET.

In this document, it is explained the steps that are required to confirm in the system side of FIs and IAPs before restarting to use CBM-NET service in the disaster situation.

The steps are as follows.

Step-2. System recovery

2-1. Damage determination and confirmation

2-2. Site change of FI's main IT system to FI's DR site and recover database if needed

2-3. Connection change to NPT-DR if CBM's site switching occurred

2-4. Connection change confirmation and informing to CBM

Each FIs and IAPs will execute these recovery steps with communicating with CBM.

2. Damage determination and confirmation

In the step of Damage determination and confirmation, each FIs/IAPs have to confirm the following things

- The availability of CBM-NET terminals in the primary site
- The availability of CBM-NET terminals in the secondary (DR) site
- The availability of Core Banking System (CBS) and FI-GW in the primary site
- The availability of CBS and FI-GW in the secondary (DR) site
- The availability of network connection to CBM-NET from the primary site.
- The availability of network connection to CBM-NET from the secondary (DR) site.

2.1 Confirmation of the availability of CBM-NET terminals

The confirmation of the availability of CBM-NET terminals will be done in both of primary site and secondary site.

As a result of confirmation, it is assumed that, at least, CBM-NET terminals in one of the sites will be confirmed as available.

2.1.1 Confirmation in the primary site

In the primary site of FIs, FIs shall confirm the availability of CBM-NET terminals. Confirmation points are as follows,

- Availability of the office space for the business operation
- Availability of the power supply
- Availability of equipment (PC) of CBM-NET terminal
- Availability of Security token and OTP token
- Availability of the image scanner for CTS (if using)

All availability is confirmed, CBM-NET terminal in the primary site is evaluated as available. If you find any unavailable things, it may be required to consider utilizing the secondary (DR) site.

2.1.2 Confirmation in the secondary site

In the secondary site, the same confirmation in the primary site shall be done and confirm the availability of equipment in secondary site.

- Availability of the office space for the business operation
- Availability of the power supply
- Availability of equipment (PC) of CBM-NET terminal
- Availability of Security token and OTP token
- Availability of the image scanner for CTS (if using)

The secondary site shall prepare in advance for the operation in case of unavailable situation of the primary site.

2.1.3 Checking Broadcast Message from CBM and reply using Inter-Bank Message

CBM will send Broadcast Message to inform the occurrence of disaster.

FIs should login to CBM-NET terminal in the primary site and check the Broadcast Message.

FIs will then send Inter-Bank Message to inform the current FIs situation.

(message sample)

<FI name> recognized Broadcast Message of disaster occurrence.

FI situation: (Please report FI situation appropriately.)

We are activating Disaster Response team.

We have activated Disaster Response team.

We are checking damage.

We have no damage.

This operation shall be referred to “6.3 Message display service” and “6.4 Inter-Bank message” in the following operation manual.

- I_Common(for FI)

Overview of procedure for Broadcast Message and Inter-Bank Message is shown below.



If it is impossible to login to CBM-NET terminal, please proceed to “2.3.1 Confirmation in the primary site”.

2.2 Confirmation of the availability of CBS and FI-GW

The confirmation of the availability of CBS and FI-GW is required to restarting to use CBM-NET with STP.

Firstly, it is assumed to confirm the status of the system in both of primary and secondary (DR) site.

- Availability of CBS and FI-GW in the primary site
- Availability of CBS and FI-GW in the secondary (DR) site

In addition, the following points are also confirmed.

- Availability of Security token for FI-GW
- Availability of connection between CBS and FI-GW

2.3 Confirmation of the availability of network connection to CBM-NET

There are some points for confirming the availability of network connection to CBM-NET.

- Availability of the network equipment for CBM-NET
- Availability of the connection to CBM-NET from CBM-NET terminal and FI-GW

FIs have to confirm above points in both of the primary site and the secondary site.

2.3.1 Confirmation in the primary site

(1) Availability of the network equipment for CBM-NET

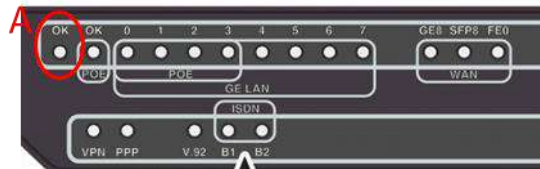
There are two type of equipment, Router and L2SW, for CBM-NET in the FIs site.

FIs confirm the availability of necessary environment for equipment, such as power supply, physical cable connection etc.

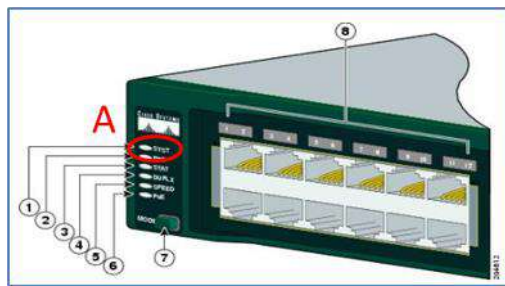
Then, FIs also confirm the availability of physical network equipment.

Please check the LED light status on the front of the Router and L2SW Devices.

Router



L2SW



If FIs found the primary equipment is unavailable, FIs confirm the availability of secondary equipment and try to switch to secondary one.

Please check the LED light status on the front of the Router and L2SW Devices as described above.

After switching to secondary equipment, please retry the step of “2.1.3 Checking Broadcast Message from CBM and reply using Inter-Bank Message” in this document.

2.3.2 Confirmation in the secondary site

FIs have to confirm the availability of network for CBM-NET in the secondary site as same as in the primary site.

(1) Availability of the network equipment for CBM-NET

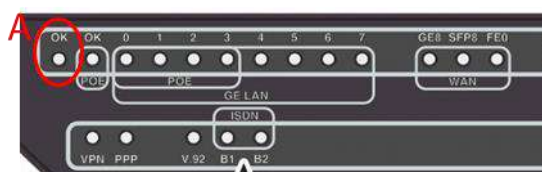
There are two type of equipment, Router and L2SW, for CBM-NET in the FIs site.

FIs confirm the availability of necessary environment for equipment, such as power supply, physical cable connection etc.

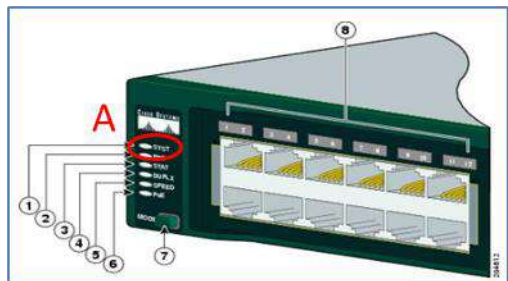
Then, FIs also confirm the availability of physical network equipment.

Please check the LED light status on the front of the Router and L2SW Devices.

Router



L2SW



If FIs found the primary equipment is unavailable, FIs confirm the availability of secondary equipment and try to switch to secondary one.
Please check the LED light status on the front of the Router and L2SW Devices as described above.

After switching to secondary equipment, please retry the step of “2.1.3 Checking Broadcast Message from CBM and reply using Inter-Bank Message” in this document.

3. Confirmation of the operation site of CBS

Which site of CBS will be utilized in the disaster situation is the matter of each FI. FIs will decide the environment in accordance with their own Business Continuity Plan (BCP) and predefined operation manual in disaster situation. The information of related with CBM-NET connection, such as the points confirmed in previous section, will be considered, when the decision is made.

After the confirmation of the CBS environment, it is assumed to confirm the following points as available for using CBM-NET.

- Availability of CBS in selected site for the operation
- Availability of FI-GW in selected site for operation
- Availability of Security token for FI-GW
- Availability of connection between CBS and FI-GW

If the case of CBM-NET site is not switched, FIs will confirm the network connection to CBM-NET in the primary site.

FIs should request CBM-NET "STP010 STP counter notification (STP010_admi009EI StaticDataRequest)" for Upstream or Downstream.

CBM-NET will return "STP010_admi010EN StaticDataReport" in response to StaticDataRequest from FIs.

If FIs receive "admin010EN", FIs can confirm that FI-GW and CBM-NET are connected and STP process is working as normal.

4. Connection change to NPT-DR

In the case of CBM-NET site is switched, it is required to change the access site for CBM-NET to NPT-DR.

After receiving the instruction by CBM, FIs have to execute necessary operation to access to NPT-DR as the operation site of CBM-NET.

FIs should request CBM-NET "STP010 STP counter notification

(STP010_admi009EI StaticDataRequest)" for Upstream or Downstream.

CBM-NET will return "STP010_admi010EN StaticDataReport" in response to StaticDataRequest from FIs.

If FIs receive "admin010EN", FIs can confirm that FI-GW and CBM-NET are connected and STP process is working as normal.

If it is impossible to connect to NPT-DR, please contact to the responsible person in CBM.

5. Connection change confirmation and informing to CBM

If FIs confirmed all required steps for connection change to NPT-DR, FIs will inform the completion status of connection change to CBM. Please contact to the responsible person in CBM.

Also, FIs have to start the confirmation of recovery points of business on CBM-NET. The necessary steps are explained in the "Disaster Recovery Manual Business operation for FIs and IAPs". FIs shall follow the instruction on it.

End of Document

Business operation for FIs and IAPs

Table of Contents

1. Overview	3
2. Confirming CBM-NET related daily operations	4
3. Resuming of business using CBM-NET terminal after system restarted.....	5
3.2 Preparation for resuming business using CBM-NET terminal	9
4. Resuming of business using STP function.....	11
4.1 Steps for recovery of business using STP after disaster	11
4.2 Recovery actions for STP	14
5. Resuming of business using File upload.....	19
5.1 Confirming restart point	22
5.2 Preparation for resuming business using File upload	22
6. Resuming business of CTS.....	24
6.1 Confirming restart point	24
6.2 Preparation for resuming business of CTS	25
Appendix-1	27

1. Overview

When a disaster occurs and YGN-CDC for CBM-NET cannot be used, the CBM-NET system will be switched to the NPT-DR site and the database will be restored by system operations.

Business processing using CBM-NET on NPT-DR will be resumed by inheriting the replicated database. Restart point using replicated database may not be the point just before when disaster occurred, there may be some lost data of completed transactions. Similarly, database recovery point in FIs/IAPs also may not be the point just before when disaster occurred.

Furthermore, this recovery point may be different between FIs/IAPs.

The recovery point of CBM-NET system will be the recovery reference point for FIs/IAPs.

Each FI/IAP must follow this recovery reference point when resuming the system process and business operations.

This Manual (DRM Business operation for FIs and IAPs) explains the process required to enable FIs/IAPs to resume business using CBM-NET system and consists of the following sections.

(1) Confirming CBM-NET related daily operations

This section explains the actions be needed after system restarted.

(2) Resuming of business using CBM-NET terminal

This section explains the steps for resuming business of using CBM-NET terminal after system restarted.

(3) Resuming of business that was processing via STP at the time of the disaster

This section explains the steps for resuming business via STP.

(4) Resuming of business using File upload

This section explains the steps for resuming business of using File upload after system restarted.

(5) Resuming of CTS

This section explains the steps for resuming business of CTS.

2. Confirming CBM-NET related daily operations

It is necessary to check how far processing has progressed in the CBM-NET daily operation schedule in CBM-NET side and FIs/IAPs' side.

As described in DRM (basic), because database recovery point may be different between CBM-NET system and FIs/IAPs, transaction(s) completed before disaster in FIs/IAPs may not be in the state of completion in CBM-NET system. Similarly, transaction(s) completed before disaster in sender FIs/IAPs may not be in the state of completion in receiver FIs/IAPs and vice versa.

FIs/IAPs should confirm what processes were completed and what processes remain to be done including completed processes that need to redo for the day.

CBM will give instruction to FIs/IAPs what should be done to resume business using CBM-NET and CTS.

3. Resuming of business using CBM-NET terminal after system restarted.

Business transaction using CBM terminal is processed by application running on CBM-NET, and it uses database on the CBM-NET system.

The database recovered after the disaster is the starting point when resuming business operations.

As described in overview, database recovered may not be same with the one just before when disaster occurred, there may be some lost data of completed transactions.

Therefore, when resuming business after database recovery, it is necessary to determine the latest transaction which was recovered.

In the following sections, the actions to be performed to confirm the restart point in business processing using CBM-NET terminal are explained using Bank to Bank Transfer as an example. Screen transitions in business processing using CBM-NET terminal are same for all businesses, so the actions to be taken before resuming business processing after completion of DB recovery after disaster will be same.

Fig3-1 and Fig3-2 shows business flow and screen transition of Bank to Bank Transfer as an example of business process using CBM-NET terminal.

Fig3-1: Example of business process using CBM-NET terminal (Business Flow)

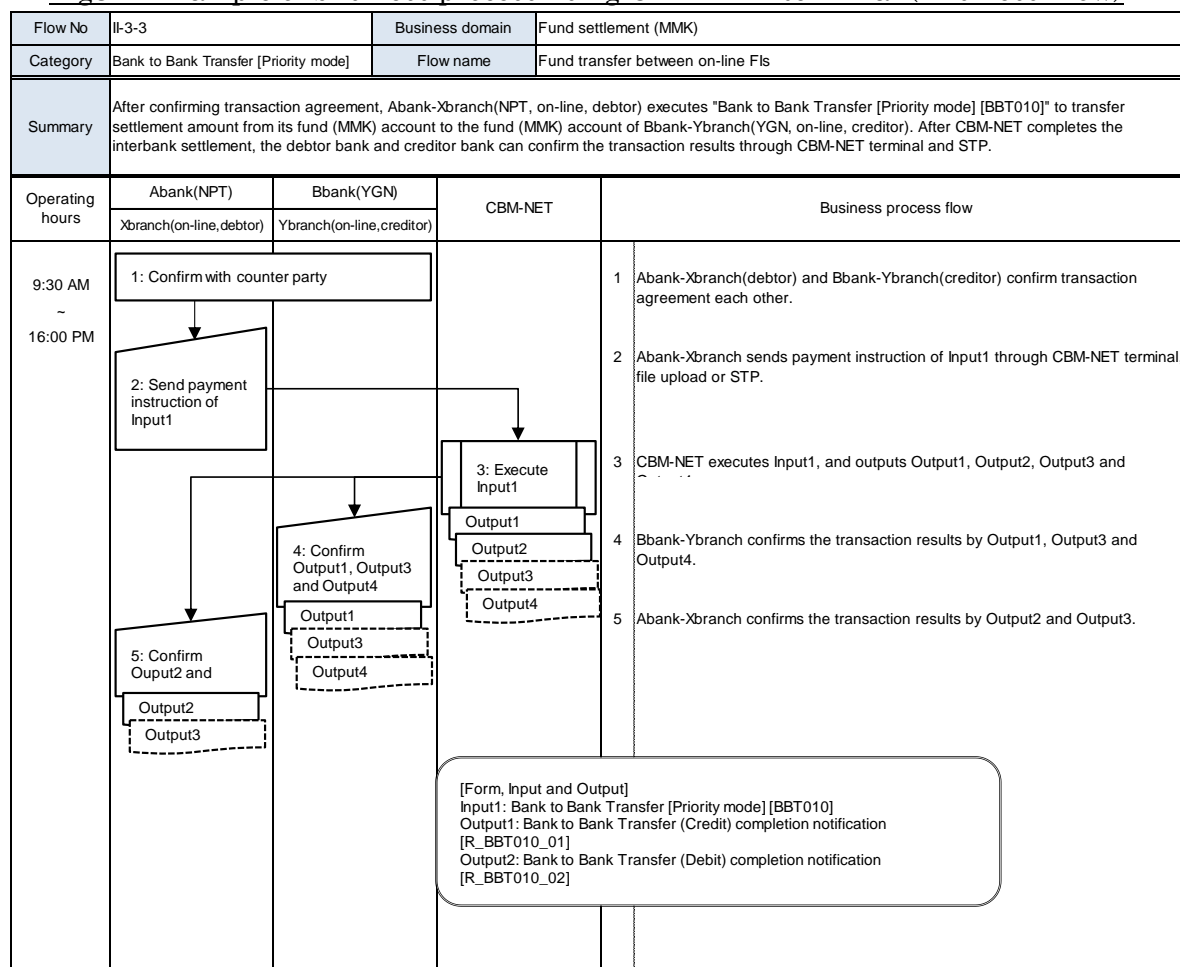
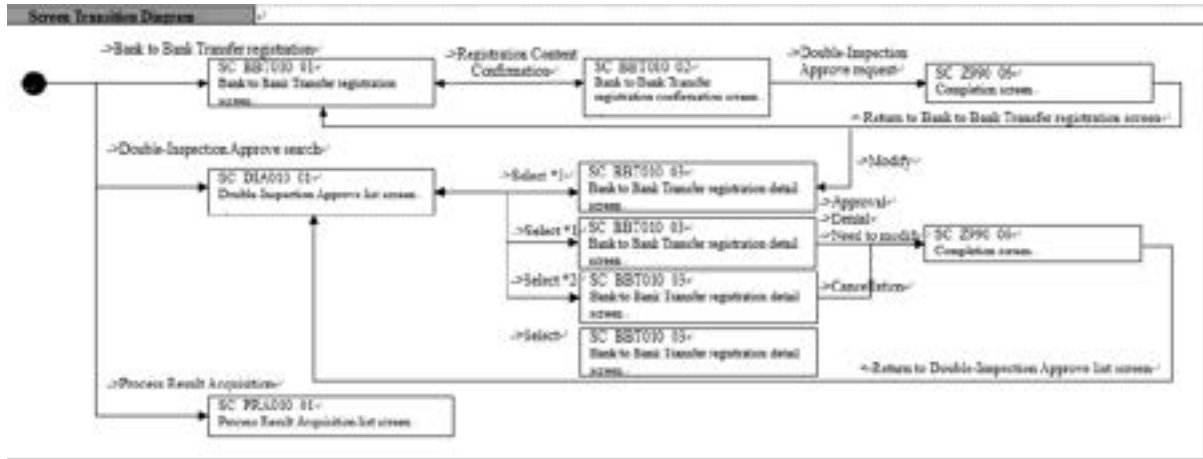


Fig3-2: Example of business process using CBM-NET terminal (Screen Transition)

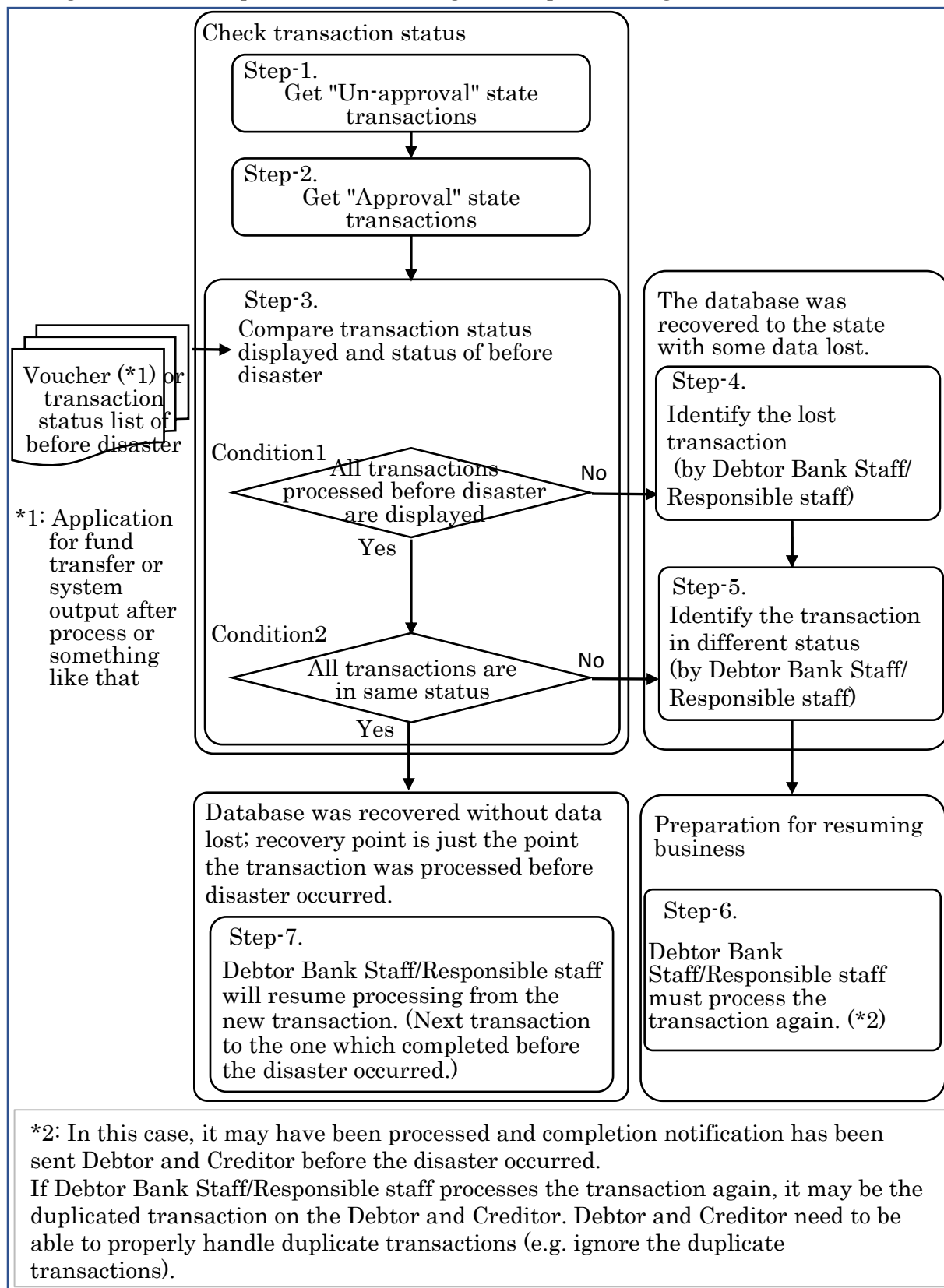


3.1 Confirming restart point

3.1.1 Step chart of “Confirming restart point”

Fig3-3 show the process step chart to confirm restart point of business using CBM-NET terminal.

Fig3-3: Process step chart of confirming restart point (using CBM-NET terminal)



3.1.2 Check transaction status

Step-1. Get "Un-approval" state transactions

- Debtor bank Staff/Responsible staff perform "Double-Inspection Approve search"("SC DIA010 01 Double-Inspection Approve list screen" with Status=Un-approval).
- Save the screen image or print the list of transaction to the paper.

Step-2. Get "Approval" state transactions

- Debtor bank Responsible Staff perform "Double-Inspection Approve search"("SC DIA010 01 Double-Inspection Approve list screen" with Status=Approval).
- Save the screen image or print the list of transaction to the paper.

Step-3. Compare transaction status displayed and status of before disaster

- Debtor bank Staff/Responsible Staff compare the transaction status displayed, transactions on the recovered database, with that of before disaster. The transaction status of before disaster can be confirmed with voucher list, status list of before disaster, application documents or transaction assignment list and/or note by staff, etc.

<Condition 1>

All transactions processed before disaster are in the "Un-approval" transaction list or "Approval" transaction list

- Case1: "Yes": go to condition 2 check
- Case2: "No": go to Step-4

<Condition 2>

All transactions are in same status of before disaster occurred

- Case3: "Yes": go to Step-7
Database was recovered without data lost.
Database recovery point is just the point the transaction was processed before disaster occurred.
- Case4: "No": go to Step-5

3.1.3 Identify transaction(s) to be reprocessed

Step-4. Identify the lost transaction

- Debtor bank Staff/Responsible Staff needs to identify the lost transaction(s).
The lost transaction(s) may be reprocessed.
- Go to Step-5

Step-5. Identify the transactions in different status

- Debtor bank Staff/Responsible Staff needs to identify the transaction(s) in different status.
The transaction(s) in different status may be reprocessed.
- Go to Step-6

3.2 Preparation for resuming business using CBM-NET terminal

When resuming business, preparations for resuming according to the situation of database recovery and the situation of the participant's system are necessary.

3.2.1 Actions to recover the transaction(s)

Step-6. Reprocess the transaction if needed

Debtor bank Staff/Responsible Staff needs to reprocess the transaction(s) identified Step4. And Step5.

- Confirm the situation of Debtor bank before reprocessing the transaction.

<Possible situation>

It may have been processed by CBM-NET application and completion notification has been sent to Debtor bank and Creditor bank before the disaster occurred.

If Debtor bank Staff/Responsible staff processes the transaction again, it may be the duplicated transaction on the Debtor bank and Creditor bank. Therefore, it is necessary to confirm the situation of Debtor bank if the status is changed from "Approval" to "Un-approval" or transactions in "Approval" status is lost.

- Actions depends on recovery status in CBM-NET.

Table3-1: Actions according to the transaction recovery status in CBM-NET

		Status of after disaster		
		"Un-approval"	"Approval"	lost
Status of before disaster	"Un-approval"	Group-1	N/A	Group-2
	"Approval"	Group-3	Group-4	Group-5

Status Group	Actions to be taken on CBM-NET terminal
Group-1	Recovered normally. No recovery action is needed on CBM-NET terminal.
Group-2	Recovered with lost data. Input transaction again and after confirming the details of the transaction, process "Double-Inspection Approve request"
Group-3	Recovered with lost data. After confirming the details of the transaction, process "Approve" (*1)
Group-4	Recovered normally. No recovery action is needed on CBM-NET terminal. (*1)
Group-5	Recovered with lost data. Input transaction again and after confirming the details of the transaction, process "Double-Inspection Approve request" and then process "Approve". (*1)
*1: Recovery action on Debtor FI's system may be needed depend on its recovery situations (refer Table3-2a and Table 3-2b)	

Table3-2-a: Classification of recovery status of Debtor FI's system

		Status in Debtor FI's system of after disaster	
		Processed according to notification from CBM-NET (camt054EN for example)	Not processed
Status in Debtor FI's system of before disaster	Processed according to notification from CBM-NET (camt054EN for example)	Group-A	Group-B
	Not processed	N/A	Group-C

Table3-2-b: Recovery actions by classification of recovery status of Debtor FI's system

Status Group	Recovery status of Debtor FI's system	Recovery actions on Debtor FI's system
Group-A	Normally recovered	No recovery action is needed
Group-B	Data lost occurred in Debtor FI's system in database recovery process	Need to recover the lost data. There is two ways to recover the lost data. 1. Create a download file that contains the data, expected to have been lost, download the created file and process according to the message in the downloaded file (*1) 2. Need to <u>request CBM-NET to resend notification from CBM-NET</u> (*2) which have been lost and process the notification from CBM-NET when receive it
Group-C	There is the possibility of 1. notification from CBM-NET have been lost before disaster occurred 2. Disaster occurred before receiving notification from CBM-NET	same as Group-B
*1: Refer to “How to create a download file for recovery” in this chapter *2: This resend request process will be described in section 4 (Resuming business using STP function)		

Step-7. Resume processing from the new transaction.

After transaction recovery process completed, Debtor Bank Staff/Responsible staff will resume processing as a normal situation.

3.2.2 How to create a download file for recovery

After system recovery, the method for FIs to check and download the processing result that exists on CBM-NET is as follows.

<Step-1>: Confirm whether the PDF file of the processing result exists

Use "Process Result Acquisition"

Get the existing processing result by one of the following methods.

- a. Get the processing result using Report Output
- b. Create Download File by File Creation and download

<Step-2>: Confirm whether or not the ACH-related processing result XML exists
(PDF file is not created for ACH-related business)

Create Download File by File Creation and download

At this time, specify the ACH-related File download subject business and Message Format ID.

<Step-3>: Perform necessary processing based on the obtained processing result

4. Resuming of business using STP function.

Restart point of CBM-NET system is the point of database restored on NPT-DR even if there are some data lost. Database here means database of CBM-NET application, not the database of CBM-NET Gateway.

The state of the database of CBM-NET application is the restarting point of the CBM-NET system.

As described in overview, database recovered may not be same with the one just before when disaster occurred, there may be some lost data of completed transactions.

Database recovery may be needed in FIs' system too.

4.1 Steps for recovery of business using STP after disaster

Steps for recovery of business using STP after disaster are shown in Fig4-1.

Fig4-1: Steps for recovery of business using STP after disaster

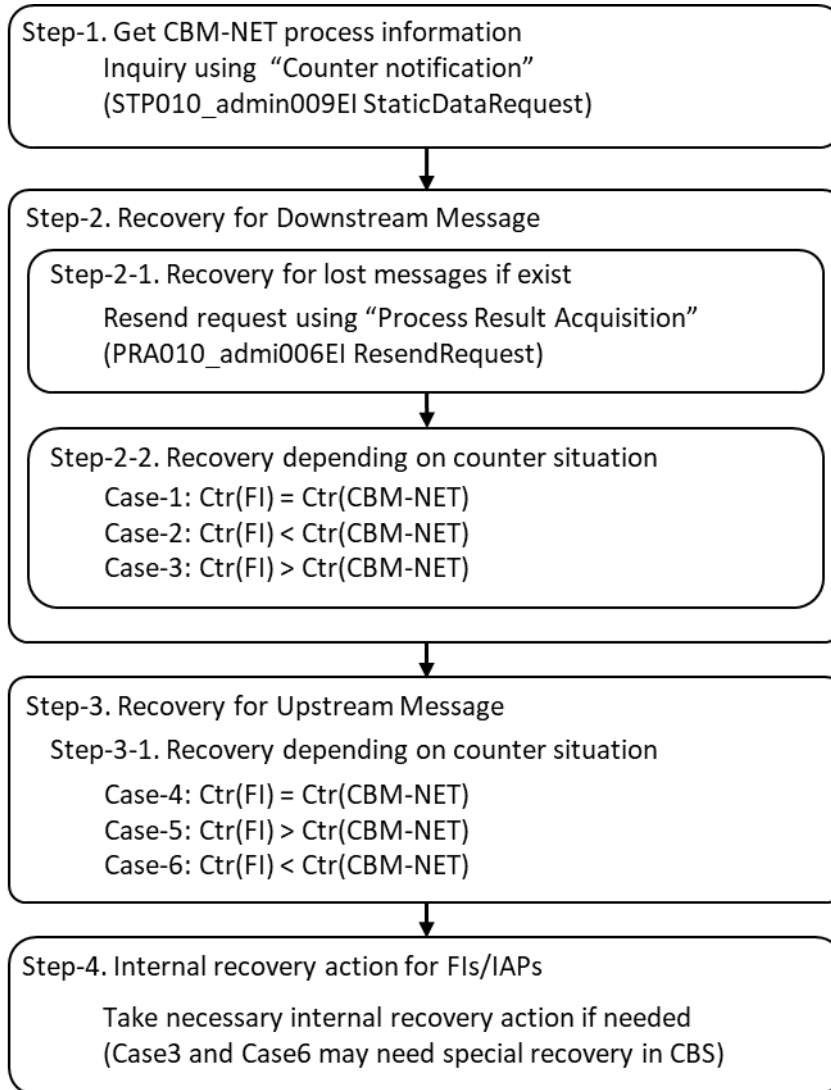
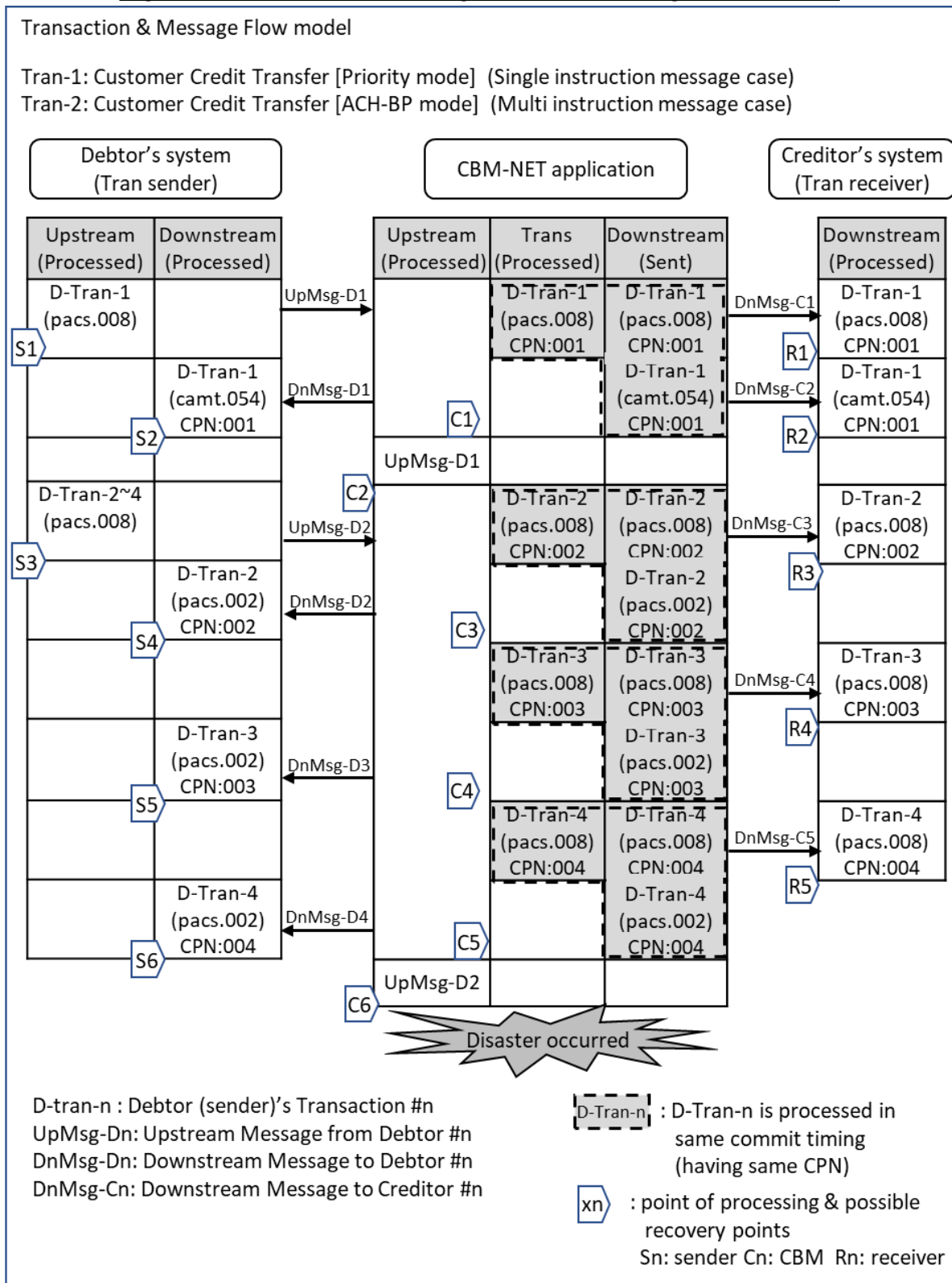


Fig 4-2 shows transaction and message flow model of CBM-NET business using STP function as an example.

Fig4-2: Transaction and Message flow model (using STP function)



C1~C6, S1~S6, R1~R6 shows the point of processing in each system.

Cn: point of processing in CBM-NET application

Sn: point of processing in Debtor FI's system (sender)

Rn: point of processing in Creditor FI's system (receiver)

If CBM-NET system received damage by disaster and YGN-CDC was switched to NPT-DR, CBM-NET system will restart with database that have been replicated to NPT-DR. Restart point of database replicated may be at C6, C5, C4,...C1 or earlier, it depends on the timing of the disaster occurred and the timing of the replication processing.

Similarly restart point of Debtor FI's system and Creditor FI's system may be at R6, S5, ...S1 and R6, R5, ...R1 or earlier.

In any case, the state of the CBM-NET database will be the point of restart.

4.2 Recovery actions for STP

4.2.1 Getting CBM-NET process information

<Step-1> Get information of message counter and message sequential number from CBM-NET

FIs can get information of message counter and message sequential number from CBM-NET by requesting

“STP010 STP counter notification (STP010_admi009EI StaticDataRequest)”.

CBM-NET returns “STP010_admi010EN StaticDataReport” containing

- Upstream (Downstream) message counter
- Sequential number part of Upstream (Downstream) message Sequential number (From) (*1)
- Sequential number part of Upstream (Downstream) message Sequential number (To) (*1)
- Sequential number part of Non existing Upstream message Sequential number list (*2)

*1: In case that there is no search result, "-(Hyphen)" is set.

*2: In case that "Sequential number part of Non existing Upstream message sequential number list" does not exist, "-(Hyphen)" is set.

FIs needs to request “STP010_admi009EI StaticDataRequest“ for “Upstream” and “Downstream” separately.

<Precautions of getting information using STP counter notification request>

There are precautions of getting information using STP counter notification request as bellow.

- Difference between using and not using search key
- When multiple “Reset times” has been used by FIs/IAPs

(1) Difference between using and not using search key

In the situation of using Upstream message sequential number as bellow,

(Sender FI)	(CBM-NET)
AAABMMMYYGNUP0000000001	AAABMMMYYGNUP0000000001
• •	• •
AAABMMMYYGNUP0000000010	AAABMMMYYGNUP0000000010
AAABMMMYYGNUP0000000011 (Lost)	(not received)

< When using search key in “STP counter notification request” >

Search key (from)= “AAABMMMYGNUP0000000001”
(to)= “AAABMMMYGNUP0000000011”

Returned value will be

Msg Counter = 10
Upstream Msg seq num (from) = “AAABMMMYGNUP0000000001”
Upstream Msg seq num (to) = “AAABMMMYGNUP0000000011”
Non existing Msg seq num list = “AAABMMMYGNUP0000000011”

< When **not** using search key in “STP counter notification request” >

Returned value will be

Msg Counter = 10
Upstream Msg seq num (from) = “AAABMMMYGNUP0000000001”
Upstream Msg seq num (to) = “AAABMMMYGNUP0000000010”
Non existing Msg seq num list = “-----”

CBM-NET had not been received “AAABMMMYGNUP0000000011” (lost message),
CBM-NET cannot return “Non existing Msg seq num list”.

(2) When multiple “Reset times” has been used by FIs/IAPs

In the situation of using Upstream message sequential number as bellow,

(Sender FI)	(CBM-NET)
AAABMMMYGNUP0000000001	AAABMMMYGNUP0000000001
. .	. .
AAABMMMYGNUP0000000010	AAABMMMYGNUP0000000010
AAABMMMYGNUP0000000011	(Lost) (not received)

(Failure occurred on FI side, “Reset times” is incremented after recovery)

AAABMMMYGNUP1000000001	AAABMMMYGNUP1000000001
AAABMMMYGNUP1000000002	AAABMMMYGNUP1000000002
AAABMMMYGNUP1000000003	AAABMMMYGNUP1000000003

< When **not** using search key in “STP counter notification request” >

CBM-NET will return “STP010_admi010EN StaticDataReport” twice

Returned value will be

Reset times = 0
Msg Counter = 10
Upstream Msg seq num (from) = “AAABMMMYGNUP0000000001”
Upstream Msg seq num (to) = “AAABMMMYGNUP0000000010”
Non existing Msg seq num list = “-----”

and

Reset times = 1
Msg Counter = 3
Upstream Msg seq num (from) = “AAABMMMYGNUP1000000001”
Upstream Msg seq num (to) = “AAABMMMYGNUP1000000003”
Non existing Msg seq num list = “-----”

In this case, FI should recognize that there may be lost message because FI sent 11 messages with “Reset times = 0” and 3 messages with “Reset times = 1”.

4.2.2 Recovery for Downstream messages

<Step-2> Recovery for Downstream messages

Do Step-2-1 and Step-2-2.

<Step-2-1> Recovery for lost message if exist

FIs should perform “ResendRequest” if there is an unreceived DownstreamMsg sequential number within the received DownstreamMsg sequential number of CBM-NET (from / to).

For all unreceived Downstream messages, issue “ResendRequest” and process the received Downstream message.

After processed the received Downstream message(s), FIs must get information of message counter and message sequential number of Downstream messages from CBM-NET.

<Step-2-2> Recovery for Downstream messages according to the message counter

Compare downstream message counter of FIs with that of CBM-NET and take recovery actions depends on counter comparison results.

Table4-1: Recovery action for each counter comparison result (Downstream)

	Counter comparison	Recovery actions
Case-1	FI = CBM-NET	No need for Downstream message recovery.
Case-2	FI < CBM-NET	For all unreceived Downstream messages, issue “ResendRequest” and process the received Downstream message.
Case-3	FI > CBM-NET	Special recovery action may be required. FI's system has already received and processed it, but CBM-NET has not processed it. (*1) It is necessary to take measures on FI's system side like a. cancelation of instruction taken according to the received downstream message. and/or b. measures on duplicate reception which may occur after resumption. Those should be done at the responsibility of each FI.
*1: Internal recovery Case-1 Case for example: FI side: S6 and CBM-NET side: C4 (refer to Fig 4-2) CBM-NET side went back to C4 where D-Tran-4 is not processed, and its process result is not reflected in the database. Of course, DownstreamMsg sequential number for Debtor's system is DnMsg-D3 and Counter is 3 in CBM-NET side.		

4.2.3 Recovery for Upstream messages

<Step-3> Recovery for Upstream messages according to the message counter

Compare upstream message counter of FIs with that of CBM-NET and take recovery actions depends on counter comparison results.

Table4-2: Recovery action for each counter comparison result (Upstream)

	Counter comparison	Recovery actions
Case-1	FI = CBM-NET	No need for Upstream message recovery
Case-2	FI > CBM-NET	<p>Send upstream messages included in "Non existing UpstreamMsg sequential number list" and messages to be processed, even if they are not included in that list, to CBM-NET.</p> <p>And process the received Downstream message as a result of upstream message sending.</p> <p>At this time, there may be a case where "TranID Duplication Error" is returned from CBM-NET.</p> <p>It is necessary to confirm the situation when received this error. (*1)</p>
Case-3	FI < CBM-NET	<p>Special recovery action may be required</p> <p>Some Upstream messages may not have been processed in FI's system, but have already been processed in CBM-NET, so it may be necessary to perform recovery processing only on FI's system side. (*2)</p>
<p>*1: Internal recovery Case-2</p> <p>Case for example: FI side: S6 and CBM-NET side: C5 (refer to Fig 4-2)</p> <p>CBM-NET side went back to C5 where UpMsg-D2 (processed) is not reflected in the database as a processed UpstreamMsg sequential number. The processed UpstreamMsg sequential number is UpMsg-D1, and Counter is 1. However, since D-Tran-2 to D-Tran-4 have been processed on the CBM-NET side, "TranID Duplication Error" will be returned.</p> <p>This should be done at the responsibility of each FI.</p>		
<p>*2: Internal recovery Case-3</p> <p>Case for example: FI side: S2 and CBM-NET side: C6 (refer to Fig 4-2)</p> <p>FI's system went back to S2 and the processing related to sending of UpMsg-D1 (D-Tran-2 ~ 4) and the post-reception processing of DnMsg-D2 ~ DnMsg-D4 are not reflected in the database of FI's system.</p> <p>The processed Upstream Msg sequential number on the FI's system side is UpMsg-D1 and Counter is 1.</p> <p>Since the post-reception processing of DnMsg-D2 to DnMsg-D4 is recovered in the processing of Step-2, it is considered that the processing related to the sending of UpMsg-D1 (D-Tran-2 to 4) is necessary.</p>		

This should be done at the responsibility of each FI.

4.2.4 Internal recovery action for FIs/IAPs

<Step-4> Take necessary internal recovery action for FIs/IAPs

If special situations, shown as “Internal recovery Case-1” ~ “Internal recovery Case-3” shown in Table4-1 and Table4-2, occur, internal recovery should be done by each FI at FI’s own responsibility.

Resuming CBM-NET related business is important to keep the method of settlement between FIs and IAPs. So, it may be considered that resuming CBM-NET related business should be done with high priority.

After taking recovery actions to resume CBM-NET related business, FIs and IAPs should do internal recovery actions depends on the situation of each FIs and IAPs.

5. Resuming of business using File upload.

Business using File upload is processed by 2 step operation, Standardized File Upload and Standardized File Upload execution.

The database recovered after disaster is the starting point of resuming business operations.

As described in overview, database recovered may not be same with the one just before when disaster occurred, there may be some lost data of completed process.

Therefore, when resuming business after database recovery, it is necessary to determine that the result of latest process before disaster is reflected in database recovered.

In the following sections, the actions to be taken to confirm the restart point in business processing using File upload are explained using Customer Credit Transfer as an example.

Fig5-1 and Fig5-2 shows business flow and screen transition of Customer Credit Transfer and file upload as an example of business process using File upload.

There are 2 concern points for the state of database recovered after disaster.

1. Uploaded file before disaster is in recovered database or not.
If the file is not in recovered database, redo of file upload is needed.
2. In case of process execution of uploaded file is stopping with “Executing processing” status. In such a situation, the processing cannot proceed with normal measures and recovery action is needed.

Actions to confirm restart point and to prepare for resume business using file upload are described in Fig 5-3.

Fig5-1: Example of business process using File upload (Business Flow)

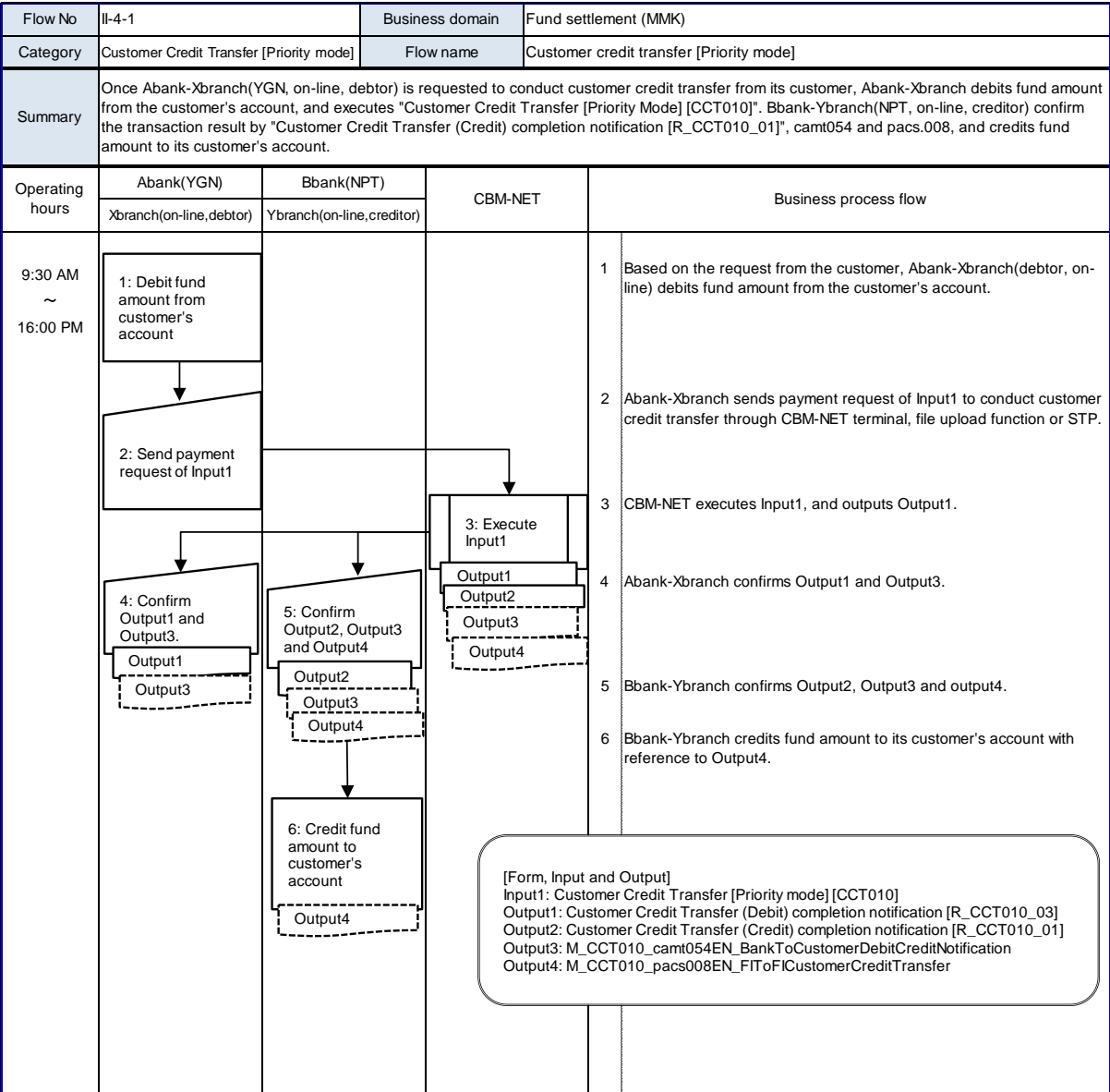


Fig5-2: Example of business process using File upload (Screen Transition)

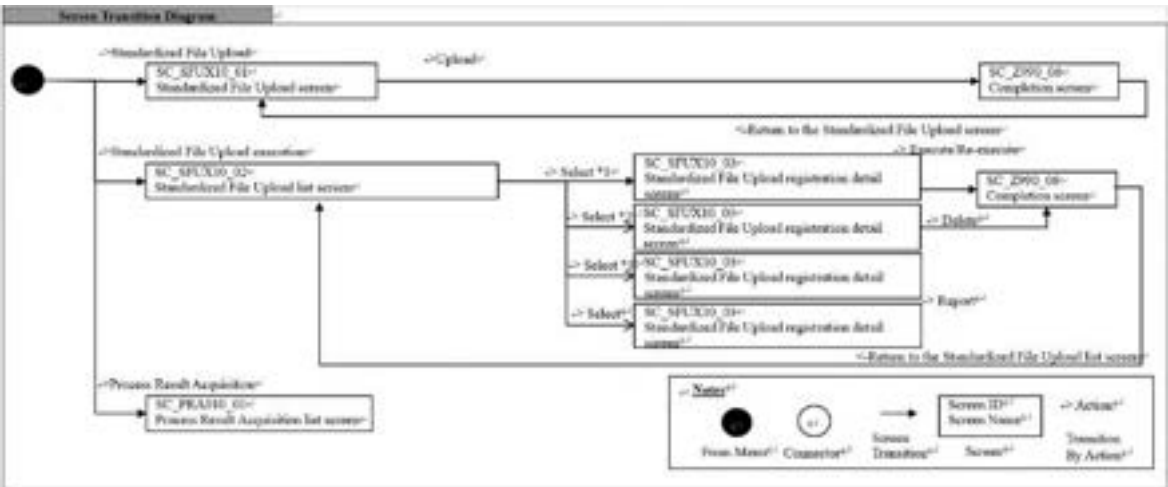
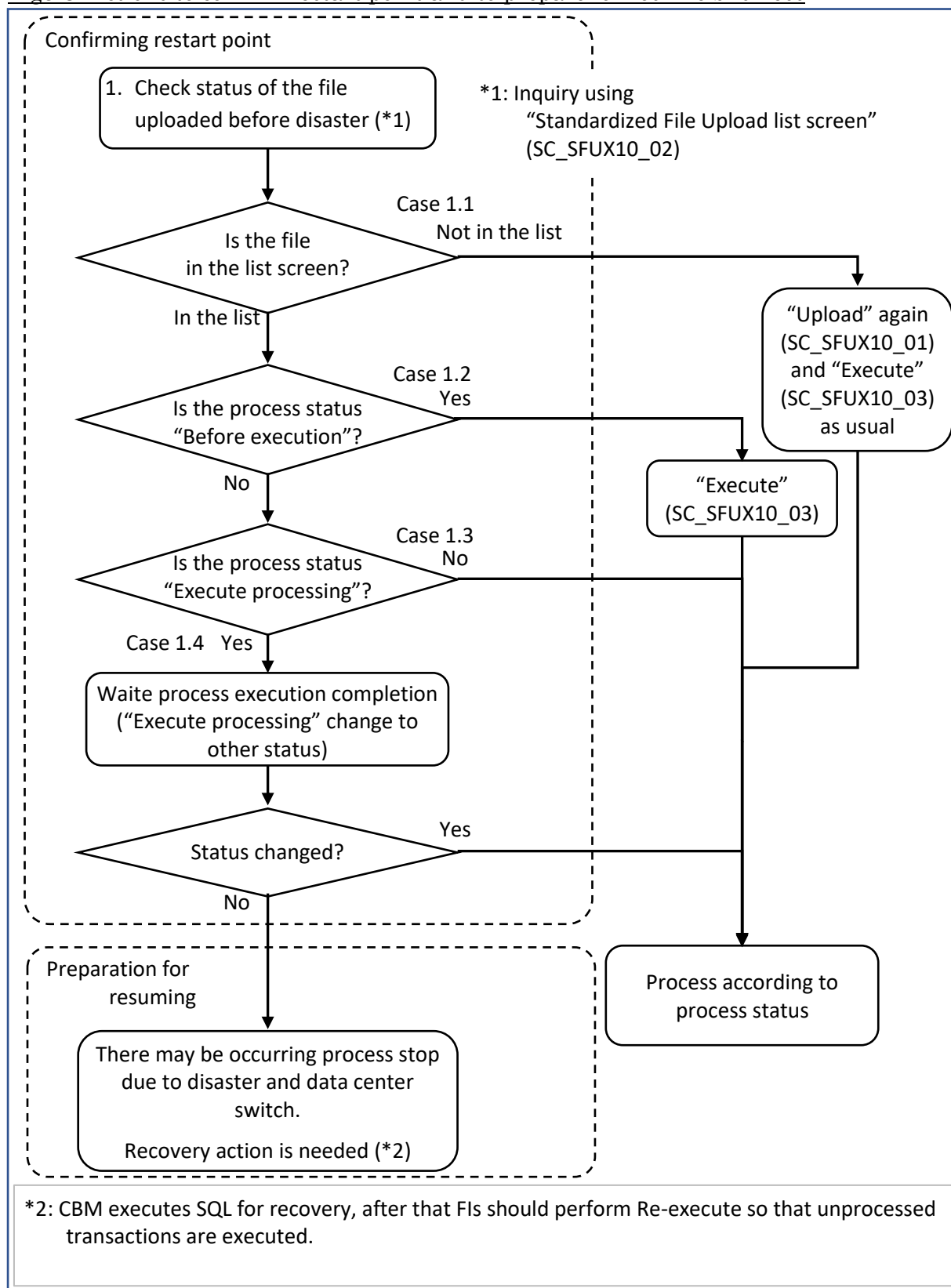


Fig5-3: Actions to confirm restart point and to prepare for resume business



5.1 Confirming restart point

Followings are the steps to confirm restart point of business using File Upload.

1. Check the process status of uploaded file before disaster by inquiry using “Standardized File Upload list screen” (“SC_SFUX10_02”).

Case 1.1. If the uploaded file is not in a screen list, database recovery point is that of before file upload completion.

Debtor bank Staff/Responsible staff needs to upload the file again (“SC_SFUX10_01”) and proceed as usual procedure (“SC_SFUX10_03” to “Execute”).

Case 1.2. If the uploaded file is in a screen list and process status is “Before execution”, database is recovered normally.

Debtor bank responsible staff can proceed “execution” (SC_SFUX10_03) and necessary process as usual.

Case 1.3. If the uploaded file is in a screen list and process status is not “Before execution” nor “Execute processing”, database may be recovered normally.

Debtor bank responsible staff can proceed necessary process according to the process status as usual.

Case 1.4. If the uploaded file is in a screen list and process status is “Execute processing”,

- a. Wait process execution completion.

But usually in this case, process execution will not complete because trigger for process to start execution is lost and process is not executing although process status is “Execute processing”.

- b. After finding out that process execution dose not finish, proceed to recovery action (Preparation for resuming).

5.2 Preparation for resuming business using File upload

In the situation of process status is “Execute processing” and the status do not change to other status, the process of “upload file execution” started by “Standardized File Upload execution” may have been stopped due to trigger for process to start execution is lost.

There is no recovery method to restart the process of “upload file execution” that was caused by data center switch in the middle of process execution.

5.2.1 Actions to proceed

To process the transactions included in the uploaded file, “Re-execute” is needed.

- CBM executes SQL to change process status to “Warning completion (Some items are not executed)”

After that, CBM inform SQL execution completion to Debtor bank staff responsible staff by using IBM010(Interbank Message) or Message display service.

- Re-execute file

Debtor bank staff / responsible staff execute the file again.
("SC_SFUX10_03" to "Execute")

5.2.2 Prerequisite for same file with new file name upload and execution

In the situation that data center switch occurred in the middle of the processing of "upload file execution", it may happen that some transactions may have been completed the process and some transactions may not have been completed the process.

This "Re-execution" of the same file may cause

"Transaction Identification duplicate error"

for the transactions which may have been completed the process before data center switch occurred.

When this error occurred, error transaction information will be outputted on PDF report. (e.g. In case of Customer Credit Transfer, R_CCT010_02_Customer Transfer upload result).

This error message can be ignored, because this may occur in disaster recovery situations.

6. Resuming business of CTS

CTS system has no remote database replication mechanism.

Basic concept of recovery after disaster is re-process.

The CTS business consists of the following three parts from the viewpoint of system processing.

1. Outward operation by presenting bank
2. Storing and clearing operation by CBM (and settlement)
3. Inward operation by issuing bank

The data flow is as follows

1. Creation of digital cheque data (Outward cheque data) by presenting bank
2. Uploading Outward cheque data to CTS web-based OCS via CBM-NET terminal by presenting bank
3. Storing digital cheque data to CTS database in CBM-NET
4. Verify Inward cheque data on web-based ICS screen via CBM-NET terminal by issuing bank

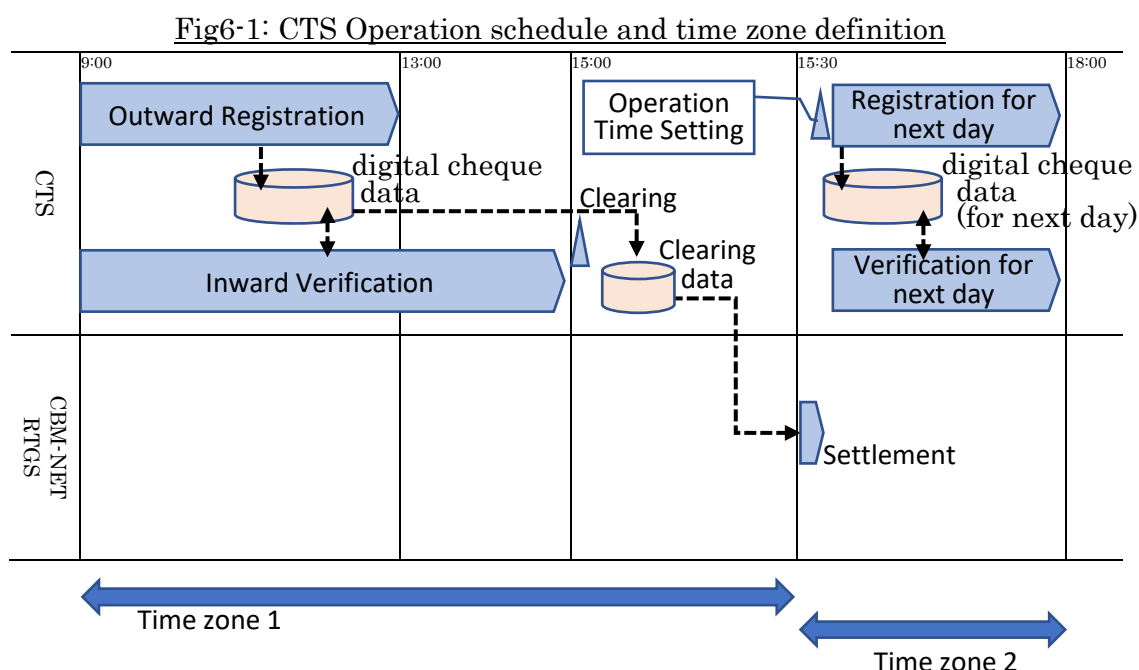
In the case of Type2 FIs, using Internal CTS, this step will be next

- Downloading Inward cheque data to CBM-NET terminal using web-based ICS via CBM-NET terminal by issuing bank.
 - Check cheque data downloaded and register the flag on Incorrect or Dishonor cheque then upload ICL file using web-based ICS via CBM-NET terminal
5. Creating clearing data at the designated time by CBM-NET CTS
 6. Feeding clearing data to CBM-NET RTGS application (settlement will be done)

6.1 Confirming restart point

6.1.1 CTS operation schedule

Operation schedule of CTS is shown as follows:



Time zone 1: From process start of the day to the point before settlement in CBM-NET completed.

Digital cheque data and clearing data are on CTS system.

Clearing data for settlement is on CTS system.

Time zone 2: From settlement in CBM-NET to end of Outward

Registration/Inward Verification for next day.

Digital cheque data for next day is on CTS system.

6.1.2 Identify the time zone on the operation schedule which disaster occurred

Because recover actions after CTS system restarted are depends on the time zone on the operation schedule, it is necessary to identify which time zone the disaster occurred.

Restart point after recovery depends on time zone is as follows

Time zone 1: <Database status>

Digital cheque data uploaded to CTS by presenting bank is lost.

(Both digital cheque data of Time zone 1 of the day and Time zone 4 of the previous business day)

Inward Verification results by issuing bank is lost.

(Both Inward Verification results of Time zone 1 of the day and Time zone 4 of the previous business day)

Clearing data created by clearing process is lost and settlement for the day is not done.

<Restart point of CTS system>

Start point of Time zone 3 of the previous business day

Time zone 2: <Database status>

Settlement for the day is done.

Digital cheque data for next day uploaded to CTS by presenting bank is lost.

Inward Verification results for next day by issuing bank is lost.

<Restart point of CTS system>

Start point of Outward Registration/Inward Verification for next day

6.2 Preparation for resuming business of CTS

To resume CTS business, recovery of CTS database is needed as a preparation for resuming business of CTS. Reprocess of Outward registration and Inward Verification will be done using CBM-NET terminal connected with NPT-DR.

Recovery actions are depending on Time zone as below:

Time zone 1: <Restart point of CTS system>

Start point of Time zone 4 of the previous business day

<Recovery action>

Presenting bank: Reprocess Outward registration from the start point of Time zone 2 of the previous business day

Issuing bank: Reprocess Inward Verification from the start point of Time zone 2 of the previous business day

Time zone 2: <Restart point of CTS system>

Start point of Outward Registration/Inward Verification for next day of today

<Recovery action>

Presenting bank: Reprocess Outward registration for next day done by today's operation

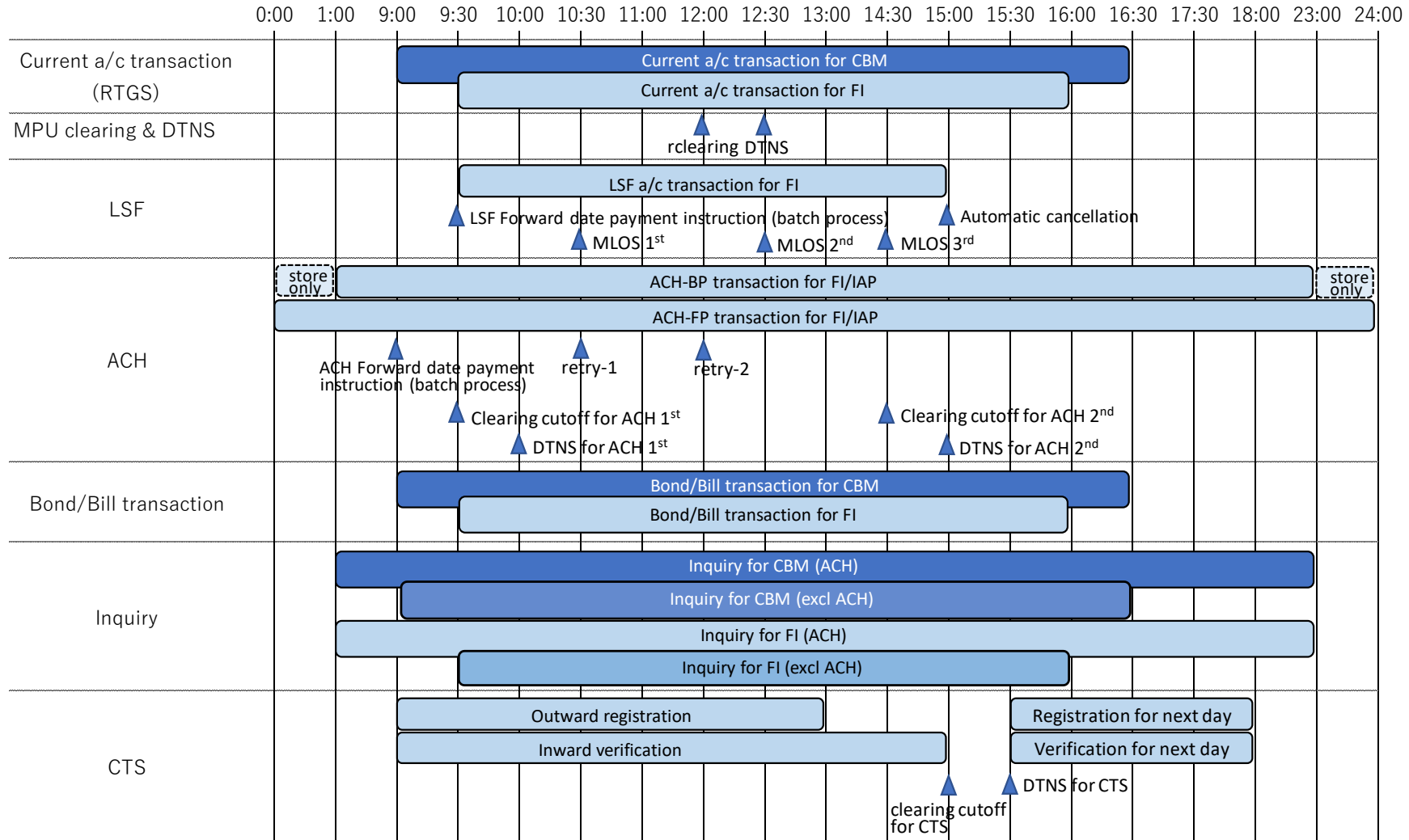
Issuing bank: Reprocess Inward Verification for next day done by today's operation

In each case, CBM will instruct participating banks the action to take for recovery of CTS system and resume business operation.

Appendix-1

Apdx1-1: CBM-NET daily operation schedule

as of 16 Nov 2020



Remarks: This schedule chart is as of 16th Nov.2020, and need to be referred latest operation schedule