Central Bank of Myanmar

Business Continuity Planning for Participants

(CBM-NET BCP)

Guidelines

Volume 2.0

(preliminary draft)

May 2021

Contents

1 INTRODUCTION

Financial institutions (FIs) could face the suspension of critical operations due to natural disasters, terrorist attacks, computer problems, and other causes. Hence FIs need to secure business continuity by formulating action plans in advance to ensure quick recovery from such suspension. There have been so many events demonstrated the need for such robust business continuity Planning (BCP) in many countries, such as the devastating Earthquakes followed by big tsunami in 2011 in Japan, the flood in 2011 in Thailand, Typhoon Haiyan in 2014 in Philippines, and the September 11 terrorist attacks in 2001 in U.S.A.

These hold true for Myanmar which has been subject to many natural disasters, including earthquakes and cyclones, and also computer problems at FIs in recent years. As a matter of fact, there is the Sagain Fault in Myanmar which could cause devastating earthquake in Mandalay, Nay Pyi Taw, and Yangon. Cyclones are becoming bigger year by year which could cause not only damages by gusts but also by floods. No one can deny the possibility having terrorists attack in Myanmar.

Most Myanmar FIs are developing core banking systems and have some form of BCP in place. However, those plans may still focus mainly on individual operating systems or facilities. Thus, in case emergency situations like the events shown the above happen, FIs need more strengthened BCP so that they can cope with even larger scale disruption than previously planned for.

This paper delineates ‘sound practice’ in terms of BCP at FIs. It should be noted at the start that individual FIs might be impacted differently depending on their location and nature of their business, and hence there could be various approaches to BCP. It should also be noted that implementation issues are still being debated, and that practical methods are evolving. Therefore, it is desirable for FIs themselves to design their own management framework that addresses their own particular risk profile, and to review such framework on an ongoing basis. The Central Bank of Myanmar (CBM) will promote discussion with FIs regarding BCP.

Section 2 gives the CBM's basic view of BCP and Section 3 details more specific and practical aspects such as how planning could be accomplished.

The participants other than FIs including indirect account participants (IAPs) such as government agencies and mobile financial service providers (MFSPs) also need to have BCP in line with the Guidelines following the instructions of CBM.

2 THE CBM' S VIEW OF BCP

2.1 SIGNIFICANCE OF BCP

BCP at FIs is deemed essential for the following three reasons:

2.1.1 MAINTAINING THE ECONOMIC ACTIVITY OF RESIDENTS IN DISASTER AREAS

BCP enables the continuation of minimum but indispensable financial services during and after disasters, thereby contributing to sustaining economic activity in a disaster area. Here disaster means Natural Disaster (earthquakes, floods, hurricanes, etc.), Man-made disaster (fires, transport accidents, industrial accidents,, terrorist attacks etc..), Technical disaster, Pandemic outbreak, etc.

The suspension of FI operations causes critical problems during and after disasters. For example, residents in a disaster area might not be able to withdraw funds, and insufficient cash on hand would prevent them from purchasing food and other necessities. Likewise, funds could not be deposited to accounts or transferred between FIs, preventing residents from receiving pension and salary payments or making payments to remote areas. Thus, FI operations are deeply intertwined with economic activity, and FIs should endeavor to continue business even in a disaster situation.

2.1.2 PREVENTING WIDESPREAD PAYMENT AND SETTLEMENT DISORDER

BCP could prevent possible defaults at individual FI caused by disasters, thereby serving to restrain widespread payment and settlement disorder. Payment and settlement services are at the foundation of economic activity and form a linked chain throughout society, with funds received as a counter value for one transaction used to pay for another. Thus, the inability of FIs in a disaster area to effect payments could see default extending beyond the area directly affected with the potential to disrupt economic activity nationwide.

BCP at FIs helps to mitigate such systemic risks.

2.1.3 REDUCING MANAGERIAL RISKS

In addition to the points above, BCP enables FIs to mitigate managerial risks.

The prolonged suspension of operations in a disaster situation makes it difficult for FIs to take profit opportunities, lowers their reputation among customers, and ultimately has a detrimental impact on their management. Therefore, BCP is necessary in terms of mitigating these risks.

2.2 KEY POINTS IN BCP

The above three points suggest FIs should have adequate business continuity plans in place. The CBM has developed business continuity plans, and it is indispensable for both FIs and CBM to coordinate their efforts in the interest of strengthening the resilience of the entire financial system. From discussions with FIs and its own experiences, CBM has identified five critical points:

2.2.1 PLANNING, TESTING, AND REVIEWING

Concrete plans should be formulated so that business can continue smoothly in the event of a disruption. Attempting to do everything right from the beginning could cause the formulation process to falter. It is more effective to start with minimal plans that can respond appropriately to a suspension of key business functions such as data centers or priority locations, and then to gradually expand to cover other operations later (phased-in approach).

Plans should be regularly tested and reviewed, if necessary, to ensure that they are practical and feasible.

2.2.2 FOCUSING ON CRITICAL OPERATIONS

Disasters result in limited access to managerial resources under severe time constraints. BCP must therefore focus on prioritized critical operations to be continued in the event of a disruption.

FIs should themselves determine what constitute critical operations according to their own business profile and management strategy. Many consider the following to be of high priority: a) cash payments to customers and acceptance of funds transfer requests, and b) large amount and high volume payment processing over the payment and settlement system.

2.2.3 CONSIDERING SPECIAL CIRCUMSTANCES UNDER LARGE SCALE DISRUPTIONS

FIs have many options for responding to disruptions and providing for business continuity, including switching over to disaster recovery center, back-up facilities, moving to manual processing, or entrusting operations to other institutions. Assuming the possibility of large-scale disruptions such as the events mentioned the above, FIs should take into consideration the following when they study options:

(1) Avoid geographical concentration of main operational offices, data centers, disaster recovery center, and back-up facilities so as to reduce risk of simultaneous damage.
(2) Be aware of the possibility that traffic suspension and other disruptions could prevent necessary staff from moving to back-up facilities.

(3) Understand that joint back-up facilities could be competed for in terms of user requests.
(4) The possibility of staff fatigue and ensuring adequate supplies because emergency conditions could continue for a prolonged period of time.
(5) Diversifying communication methods because ordinary telecommunications may be suspended or severely restricted.

2.2.4 COORDINATING BCP WITH OUTSIDE PARTIES

The operations of FIs are deeply intertwined. It is thus desirable that institutions coordinate with other market participants, payment and settlement system operators, and outside service providers in order to increase the effectiveness of their own BCP. Such coordination ultimately strengthens the resilience of the entire financial system. It is important in this context to mutually disclose information regarding BCP status and contact points in an emergency within predefined limits and with adequate information security.

2.2.5 EXERTING STRONG LEADERSHIP

BCP is a major project that requires the substantial investment of managerial resources and a FI-wide awareness. Management needs to exert strong leadership and to become deeply involved in the process. Management should be in the role of CEO (Chief Executive Officer), CTO (Chief Technology Officer), or other relevant position.

3 PRACTICAL ASPECTS OF BCP

The process of BCP outlined below may be followed by FIs in formulating BCP. This section considers the practical aspects of each step.[1]

BCP consists of five processes, (1) Formulating a framework for robust project management, (2) Identifying assumptions and conditions for BCP, (3) Identifying business impact, (4) Introducing action plans, and (5) Testing and reviewing.

(1) Formulating a framework for robust project management consists of (i) Basic policy, (ii) FI-wide control section, and (iii) Project management procedures.
(2) Identifying assumptions and conditions for BCP consists of (i) Disaster scenarios, (ii) Critical functions & operations, (iii) Recovery time objectives, and (iv) Recovery point objectives.
(3) Identifying business impact such as the availability of business/operation and non-availability of business/operations (e.g. stop daily cash collection, new business product request, etc.)
(4) Introducing action plans consists of (i) Business continuity measures, (ii) Robust back-up data, (iii) Procurement of managerial resources, (iv) Decision-making procedures and communication arrangements, and (v) Practical manuals.
(5) Testing and reviewing, and Other issues will also be described. BCP should be updated as necessary.

3.1 FORMULATING A FRAMEWORK FOR ROBUST PROJECT MANAGEMENT

3.1.1 BASIC POLICY

FI management should develop basic policy and guidelines for BCP and provide details FI-wide. These documents should clearly state the need for BCP, the concepts to be used in identifying critical operations, and the executive officer in charge of initiating the plans. This formulation encourages the organization to become more aware of the need for crisis management and to implement subsequent work more efficiently. The detailed scope of BCP manual should be developed by FIs based on their requirements. Some detailed scope BCP related with Cheque Truncation, Automated Clearing House, Switching Main Data Center to Disaster Recovery System can also be referred at each respective manuals.

The backup policy is shown as follows: (i) automatically backup as much as possible, (ii) in principle, the backup process being centrally managed by Backup Server, (iii) using shared storage for primary backup and linear tape-open (LTO) for secondary backup, (iv) obtaining two generations

[1] This paper focuses on aspects related to business operation. Other aspects such as announcements to the press and disseminating information to customers are also essential.

of backups for each shared storage and LTO medium, (v) adopting volume copy function to storage-to-storage backup, and (vi) LTO backup being performed from backup data in the shared storage as well as the tape backup being performed while the business continues.

Recovery policy is shown as follows: (i) in principle, data being restored from backup data in backup area, (ii) in case of all storage being failed, system data being restored from LTO tape, and (iii) equipment which may fail needs to be recovered based on the specified procedures.

3.1.2 FI-WIDE CONTROL SECTION

BCP requires FIs to study FI-wide aspects. From this point of view, it is desirable that a FI-wide control section is designated and/or officer in charge appointed. The section is responsible for formulating specific work procedures, assigning work to individual departments, and coordinating among departments based on the policy and guidelines. In addition, the section could plan and carry out testing programs after the plans are set up and conduct regular review thereafter.

3.1.3 PROJECT MANAGEMENT PROCEDURES

BCP is an extremely difficult project that involves a large number of interested parties. This difficulty requires FIs to implement appropriate progress control, including reports to top management. Specifically, FIs must have a mechanism by which the FI-wide control section can monitor work progress and report to management so that they make decisions in a timely and flexible manner on additional resources and work priorities. BCP related projects are generally managed by a department responsible for Payment and Settlement System including its business operations. Having said that, BCP projects are related to a variety of activities which could have serious impact on the bank-wide operations. As such, the department is requested to coordinate and cooperate with other departments including IT department, cash management department, other business operation department, policy department, etc. playing the role as the secretariat for the BCP projects. The department also needs to plan and prepare for the test (drill) regularly to make BCP plan work appropriately in case of emergency. Also, the responsible department should report to the top management of each bank regularly and timely as mentioned the above. The responsible department for BCP projects in each bank needs to report to CBM regularly and timely as well when any changes happen with respect to the BCP related issues.
Note: Annex I Duties and Responsibilities of each responsible person designated by FI for BCP related issues is attached for reference. FIs can develop its own structure based on its organization chart.

3.2 IDENTIFYING ASSUMPTIONS AND CONDITIONS FOR BCP

3.2.1 DISASTER SCENARIOS

(1) Recognition of potential threats

Following are types of disasters that could pose threats to financial institution operations: (i) natural disasters such as earthquakes and typhoons, (ii) man-made disasters such as terrorism and computer crime, (iii) technical disasters such as power outages and computer problems, and (iv) a pandemic outbreak of an infectious disease such as Sever Acute Respiratory Syndrome (SARS) and Coronavirus disease 2019 (COVID-19). Individual financial institutions need to identify potential threats, given circumstances such as the location and nature of their business.

(2) Analysis of frequency and severity

The next step is to analyze the frequency of potential threats that could emerge as well as the severity should they emerge. This analysis specifically refers to assuming the extent of the damage to offices and data centers caused by disasters and considering how the operations of FIs could be suspended as a result. It is also necessary to evaluate the consequent damage stemming from such events as payment delays, and funding difficulties. In this analysis, FIs should also consider the impact on their customers and other FIs.

(3) Identification of material risks and damage scenarios

Having analyzed potential threats and their severity, FIs should identify specific scenarios with material risks. Business continuity planning should be developed based on these specific scenarios.

The following scenarios are to be considered: (i) stoppage of computer systems due to a disaster which strikes the data center, (ii) loss of head office functions due to a disaster which strikes the head office, (iii) simultaneous suspension of operations at multiple locations due to a major earthquake, (iv) a pandemic outbreak of an infectious disease, (v) loss of staff, (vi) limitation of transport and restriction of access to public building, and (vii) degradation of service level.

3.2.2 CRITICAL FUNCTIONS AND OPERATIONS

Disasters result in limited access to managerial resources under severe time constraints. Therefore, in the event of a disruption, FIs should focus on continuing prioritized critical functions and operations. It is a general recognition that many FIs consider the following examples as critical operations: (i) cash payments to customers and acceptance of funds transfer requests, and (ii) large amount and large volume payment processing over the payment and settlement system. Extra attention is needed in the handling of ‘unsettled transactions’ when prioritizing the operations above (refer to the following note). When deciding the critical functions and operations, FIs may consider the minimum service level, critical business functions, and Non-IT & IT resources as well as other alternative

resources that can still be accessed in case of some emergency situation. Critical functions and operations decided by FIs should be reported to CBM.

Note: Unsettled Transactions

'Unsettled transactions' refers to transactions that have been accepted but where processing has not been completed at a certain point in time. When computer systems fail and operation is resumed manually, it is necessary to determine whether individual transactions should be reprocessed. Otherwise, insufficient manual operations could increase the risk of double processing or failure to process. 'Unsettled transactions' could occur when several system processes must be completed, in case of disaster. For example, an operator accepts a transaction for processing, manages due dates, and effects settlement. Unless the data is transferred among processes instantaneously, there is the potential for an 'unsettled transaction' to occur. When accepting data, the data may stay in a queue for a certain period of time. In case the data are for future dated transactions such as payroll data, the data could stay in a queue for several days before completely processed and finally settled. As such, "unsettled transactions" could occur and need to be handled appropriately.

3.2.3 RECOVERY TIME OBJECTIVES (RTO)

Based on the necessity of operations, FIs set target times for the resumption of operations by provisional means such as processing at a disaster recovery site. These targets need to include estimates of the time required to (i) switch to back-up systems, (ii) correct data needed for on-line resumption, and (iii) move staff. For reference, major FIs in leading countries generally plan to resume critical operations such as large amount and high-volume settlements within two to four hours assuming that 'main facility functions are suspended, but transportation and other infrastructure are available and there is no human damage.' Therefore, RTO for operations related with CBM-NET services such as Funds Transfer Service (FTS), Central Securities Depository (CSD), and Automated Clearing House (ACH) is to be 2 hours.

3.2.4 RECOVERY POINT OBJECTIVES (RPO)

CBM-NET services such as FTS, CSD, and ACH are backed up from main center to disaster recovery site by a real-time replication. Therefore, RPO for the services are near zero. With respect to the CTS, data are backed up daily to be recovered from the previous day. As such, cheques need to be re-entered (scanned again) from the start of the day when disaster happened.

3.3 INTRODUCING ACTION PLANS

3.3.1 BUSINESS CONTINUITY MEASURES

The next step is to study specific measures for the plan based on determined assumptions and conditions for BCP. These measures should take account of the volume of clerical processing involved, the time required per transaction, and due date times for completing operations on the day of disaster. Based on this study, FIs determine whether back-up facilities should be used, whether manual processing is required, or whether additional staff are needed.

3.3.2 ROBUST BACK-UP DATA

Regardless of the means by which operations continue, data recorded before a disaster is indispensable for quickly resuming operations. This requires a mechanism for acquiring and maintaining data back-ups. FIs must identify the information required to resume critical operations, for example, raw transaction data, ledger update data, balance sheet data, and uncompleted transaction details. Then, they must acquire and maintain this back-up data in electronic or paper form.

Particularly important back-up data is generally transported by magnetic tape or transmitted by telecommunication lines to remote storage locations. In this case, however, it is critical to ensure that back-up data can be easily obtained during times of disaster. Some FIs maintain back-up data in back-up facilities, and others have printers specifically for data output installed in their operational centers or head office payment and settlement departments.

3.3.3 PROCUREMENT OF MANAGERIAL RESOURCES

(1) Managerial resources
FIs determine the processing capacity required for continuity of critical operations regarding staffing, computer capacity, and telecommunication capacity. To meet this requirement, they provide adequate resources such as staff, IT equipment, and telecommunication lines.

(2) Public infrastructure availability
Operations are conducted based on the assumption that electricity, gas, water, transportation, telecommunications, and other public infrastructure can be used. Thus, BCP should take account of the availability of infrastructure in an emergency.

3.3.4 DECISION-MAKING PROCEDURES AND COMMUNICATION ARRANGEMENTS

(1) Decision-making procedures and command structure

Disasters impose strong time constraints on emergency decisions. Thus, FIs need to predetermine decision-making procedures and command and reporting lines. Currently, in many FIs, management has to confirm a state of emergency and then establish a 'crisis management team' or other disaster management organization such as "disaster countermeasures office" headed by a designated executive in head office (or an alternative location if the head office must be evacuated). In most cases, their functions tend to be centralized to collect information and make decisions.
It may not be possible to contact top management or department heads in the event of large scale disruption. Thus, it is desirable that financial institutions have management systems that ensure the smooth delegation of authority in such a situation.

In case of disaster, unforeseeable events which can't be covered by BCP guideline and manuals could happen. In such a case, responsible persons for BCP need to decide and manage situation based on their capacity appropriately.

(2) Emergency contact lists and emergency communication means
Communication among responsible parties is essential to initiate an appropriate response to disasters. FIs must have emergency contact lists for Government Bodies and other responsible parties such as crisis management team, employees, customers, media, etc. and provide emergency means of communication [Annex II Notification of contact person for BCP related issues and Annex III Notification of responsible person for BCP related issues]. It is highly likely, however, that fixed line telephones, facsimiles, and mobile telephones may be suspended or subject to restrictions in the event of large scale disruption. Therefore, it is desirable to prepare several different means of communication. In case of emergency situation, the Internet including e-mail and mobile wireless proved particularly effective. With respect to the Emergency Means of Communication used by FIs, refer to the following Note.

Note: Emergency Means of Communication Used by FIs

Possible means of communication to be used by FIs in case of emergency are as follows: (i) Fixed telephone line, (ii) Mobile telephone, (iii) E-mail (Internet mail, mobile mail), (iv) Priority telephone service for use in emergencies, (v) Direct hotlines, (vi) Wireless (mobile wireless, disaster wireless), Satellite telephone(vii) Telephone conferencing system, (viii) Video conferencing system, (ix) Internal broadcasting system, (x) Employee safety confirmation system (uses telephone or e-mail), (xi) Internal notification and automated broadcasting system to all employee homes or other registered telephone numbers (uses telephone, facsimile, and/or e-mail), and (xii) An emergency web site which employees can access from outside.

3.3.5 PRACTICAL MANUALS

Formulating practical and easily understood manuals regarding operational procedures for each department level is an effective way of ensuring the feasibility of BCP. Some FIs store copies of manuals of other related departments for better coordination among related departments.

3.4 TESTING AND REVIEWING

Implementation of testing/training programs on a regular basis is essential to ensure the feasibility of BCP. It is desirable to conduct testing/training programs at least annually. Testing/training indicates whether recovery time objectives can be achieved, identifies challenges, and enables FIs to review the adequacy of equipment that is used only in the event of a disruption. There are various testing/training programs. For example, it may be difficult to conduct testing/training in which all relevant departments participate. In this situation, testing/training could be limited to specific points to be verified or a specific range of participants. It is also worth considering testing/training programs with outside parties with which the financial institution exchanges a large volume of data. As reference, CBM holds annual testing/training sessions for CBM-NET participants, including those directly connected with straight through processing (STP), in order to confirm switch over to the CBM-NET disaster recovery site. Some examples of testing and training programs are shown as follows:

Note: Examples of Testing/Training Program

Followings are examples of testing/training programs. For more detailed cases (scenarios), please refer to the Business Manuals.

(1) Communications system testing/staff movement training

The communications system testing/staff movement training consists of (i) Decision-making and communications system which is described as "'Crisis management team' or other risk management organization formed, communications procedures verified and learned"; (ii) Evacuation which is described as "Procedures for evacuating from buildings verified and learned assuming bomb threat or fire"; and (iii) Relocation which is described as "Procedures for moving staff from main facilities to back-up facilities verified and learned as well as Relocation procedures when public transportation is unavailable (walking or cycling from home) verified and learned".

(2) System operation testing/business operation training

The system operation testing/business operation training consists of (i) Back-up equipment start up which is described as "Start-up procedures for back-up computers and equipment not normally used verified and

learned; (ii) Disaster recovery site switch over which is described as “Procedures for switching from main center to disaster recovery site verified and learned; (iii) Manual operation which is described as “Operational procedures for system failure and telephone network failure (manually written document transactions and provisional payments, etc.) verified and learned; and (iv) Rotation which is described as “Operational procedures including terminal input verified and learned during a full day of actual work at back-up facilities”.

Based on the tested results, BCP in particular action plans are to be reviewed and updated if necessary. New BCP should be reported to CBM.

3.5 OTHER ISSUES

3.5.1 PRECLUDING AND MITIGATING DISASTER DAMAGE

Many disaster risks and damage could be prevented or mitigated through prior measures to some extent. Therefore, FIs need to take steps to prevent risks from materializing, in conjunction with the introduction of BCP. Examples of efforts seen at FIs are as follows: (i) establishing facilities at or moving them to relatively low-disaster risk locations, (ii) anti-seismic retrofitting, (iii) installation of back-up generators, (iv) enhancement of access control to restricted areas, (v) strengthening of firewalls to prevent hacker attacks, etc.

3.5.2 LOCATION OF BACK-UP FACILITIES

It is desirable to choose a back-up facility location that is far enough to avoid being affected by any disaster which could threaten the main facility. Otherwise, it might be subject to the same disaster. It is particularly important that back-up facilities do not share telecommunication lines or electric power supply routes with main facilities.
Likewise, it is also necessary to take account of staffing requirements when locating back-up facilities. This is particularly the case where plans call for main facility staff to move to the back-up facility. Institutions should examine the feasibility of plans in the event of a large-scale disruption.

3.5.3 USE OF OUTSIDE SERVICE PROVIDERS

FIs could provide their own back-up facilities or rely on outside service providers. Many providing their own facilities utilize not only traditional methods such as dedicated facilities, neighboring locations, and other operational centers, but also others such as having some staff work at home so that enough space can be secured for emergency staff. FIs depending on outside service providers sign contracts for emergency facilities with service providers, and/or entrust operations to their affiliates or other FIs.

When using outside service providers, FIs should be aware of the need to obtain sufficient information from the service provider regarding the potential for competition with other customers. In fact, when FIs faced suspension of critical operations due to emergency situations, it was reported that there was excessive demand for the facilities of outside service providers.

ANNEX I : DUTIES AND RESPONSIBILITIES OF EACH RESPONSIBLE PERSON DESIGNATED BY FI FOR BCP

No	Responsible Person	Duties and Responsibilities
1	CEO	- is a BCP Leader. - is responsible for arranging emergency plan. - is responsible to appoint a second leader for every branch/sector, in case of emergency, for Business Continuity. - is responsible for developing own BCP manual in line with BCP guideline. - is responsible for cooperating with CBM.
2	Business Function Leader/Manager	- is responsible for cooperating with the responsible person of Payment and Settlement Department in Central Bank of Myanmar. - is responsible for prioritizing critical operations by computerized system. - is responsible for planning the scenario that can be done manually.
3	Business Operation Team	- is to conduct BCP from business perspective in line with basic policy, firm-wide control measures, project management procedures, etc. - is to identify assumptions and conditions for business continuity planning including disaster scenarios, critical operations, recovery time objectives, etc. - is to introduce action plans including business continuity measures, robust back-up data, procurement of managerial resources, decision-making procedures & communication arrangements, practical manuals, etc. - is to test and review the above issues cooperating with IT Operation Team.
4	IT Operation Leader	- is responsible for making drill in line with BCP guideline and Disaster Recovery manual. - is responsible for switching Data Center/Disaster Recovery (DC/DR). - is responsible for implementing DR System for backup and manual operations in case of emergency. - is responsible for cooperating with IT Department, Central Bank of Myanmar.
5	IT Operation Team	- is to start-up back-up systems and facilities and to switch over to them. - is to test and secure operational procedures of back-up systems and facilities in case of emergency. - is to start-up back-up networks and switch over to them. - is to test and secure operational procedures of back-up networks in case of emergency
6	Emergency Contact Person	- is a Contact Person and Responsible Person mentioned in Annex I and II to contact with CBM in emergency for BCP & DR Switching

*Note: This is the reference for duties and responsibilities of BCP for FIs. FIs needs to develop its own structure based on its organization chart.

ANNEX II NOTIFICATION OF CONTACT PERSON FOR BCP

To:	The Director General Central Bank of Myanmar	
From:	Name of Institution (FI, etc.):	
	Myanmar Company Registration Number:	
	Registered Office Address/Principal Place of Business in Myanmar:	
	BIC:	
	Name of contact person for BCP:	
	Position and department of the person	
	Telephone Number:	
	Fax Number:	
	E-mail:	
	Starting date:	
	Name of alternate person for BCP:	
	Position and department of the person	
	Telephone Number:	
	Fax Number:	
	E-mail:	
	Starting date:	
	Note: if there is any predecessor who will be replaced by the person, describe the name of the predecessor and the reason:	

ANNEX III NOTIFICATION OF RESPONSIBLE PERSON FOR BCP

To:	The Director General Central Bank of Myanmar	
From:	Name of Institution (FI, etc.):	
	Myanmar Company Registration Number:	
	Registered Office Address/Principal Place of Business in Myanmar:	
	BIC:	
	Name of responsible person for BCP:	
	Position and department of the person	
	Telephone Number:	
	Fax Number:	
	E-mail:	
	Starting date:	
	Name of alternate person for BCP:	
	Position and department of the person	
	Telephone Number:	
	Fax Number:	
	E-mail:	
	Starting date:	
	Note: if there is any predecessor who will be replaced by the person, describe the name of the predecessor and the reason:	