Common Understanding on Cross-Border Business Continuity Planning and Cybersecurity

Cross-Border Settlement Infrastructure Forum

ADB

Common Understanding on Cross-Border Business Continuity Planning and Cybersecurity

Cross-Border Settlement Infrastructure Forum


Creative Commons Attribution 3.0 IGO license (CC BY 3.0 IGO)

6 ADB Avenue, Mandaluyong City, 1550 Metro Manila, Philippines
Tel +63 2 632 4444; Fax +63 2 636 2444
www.adb.org

Publication Stock No. ARM189299-2

Notes:
In this publication, "$" refers to US dollars.
ADB recognizes "Korea" as the Republic of Korea, and "Hong Kong" as Hong Kong, China.
Corrigenda to ADB publications may be found at http://www.adb.org/publications/corrigenda.

Contents

Acknowledgments	iv
Statement from the Cross-Border Settlement Infrastructure Forum Chair	v
Overview	vi
Introduction	1
Cross-Border Central Securities Depository-Real-Time Gross Settlement Linkages	2
The Importance of Cross-Border Business Continuity Planning and Cybersecurity	4
Common Understanding on Cross-Border Business Continuity Planning and Cybersecurity Frameworks	6
Next Steps	8

Acknowledgments

The Asian Development Bank (ADB), as Secretariat of the Cross-Border Settlement Infrastructure Forum (CSIF), would like to express its sincere appreciation to the chair and vice-chair for guiding the discussion, and to members and observers for providing inputs to the Common Understanding on Cross-Border BCP and Cybersecurity.

The objective of this report is to create a common understanding among CSIF members on the importance of business continuity planning and cybersecurity frameworks as they work toward realizing central securities depository and real-time gross settlement linkages. The report should be regarded as a crystallization of regional collaborative efforts and knowledge toward more harmonized and integrated Association of Southeast Asian Nations, the People's Republic of China, Japan, and the Republic of Korea (ASEAN+3) bond markets through CSIF activities. Without the strong support and cooperation of CSIF members and observing authorities in the region, this report would not have been published.

This report does not represent the official views of ADB or any of the institutions that participated as CSIF members or observers.

The ADB Secretariat expresses its sincere gratitude to CSIF members and observers.

Statement from the Cross-Border Settlement Infrastructure Forum Chair

As the vice-chair of the Cross-Border Settlement Infrastructure Forum (CSIF), and in my capacity as acting chair of the CSIF, I would like to express our heartfelt gratitude to members and observers for their contributions toward the success of this initiative. The publication of the Common Understanding on Cross-Border Business Continuity Planning and Cybersecurity undoubtedly comes at the right time given the increasing number of cyber threats around the world. As the operators of financial market infrastructure, it is important that our systems are resilient to all types of cybercrimes and unexpected or unforeseeable natural disasters.

I hope to receive the continuous support of CSIF members and observers for this initiative since this report is only the first stage in bringing the objectives of the CSIF to fruition. On behalf of all CSIF members and observers, I would like to express our sincerest appreciation to Bella Santos, former Director of the Payments and Settlements Office, Bangko Sentral ng Pilipinas, who served as CSIF chair until November 2017, for her guidance and efforts in compiling this publication.

Seung-Kwon Lee
Vice-Chair, CSIF
Acting Chair, CSIF
Director
Korea Securities Depository

Overview

The Asian Bond Markets Initiative (ABMI) Task Force 4 has conducted several studies on a Regional Settlement Intermediary (RSI), including one carried out by the Group of Experts (GOE) and a subsequent reassessment of the GOE's legal and business feasibility study. The Cross-Border Settlement Infrastructure Forum (CSIF) was established at the meeting of finance ministers and central bank governors of the Association of Southeast Asian Nations (ASEAN), the People's Republic of China, Japan, and the Republic of Korea—collectively known as ASEAN+3—in May 2013 in Delhi to further the work of GOE.

The CSIF was mandated to facilitate discussion on the improvement of cross-border bond and cash settlement infrastructure in the region, including the possibility of establishing an RSI. The CSIF aims to (i) enhance dialogue among policy makers and operators of bond and cash settlement infrastructure in the region; (ii) assess the existing settlement infrastructure and identify comprehensive issues and requirements to facilitate cross-border bond and cash settlement infrastructure in the region; (iii) develop common basic principles for cross-border bond and cash settlement infrastructure with a medium- and long-term perspective; and (iv) discuss prospective models, an overall roadmap, and an implementation plan for establishment of cross-border bond and cash settlement infrastructure in the region. Central banks and national central securities depositories (CSDs) in ASEAN+3 participate in the CSIF on a voluntary basis. The CSIF reports to the ABMI (Task Force 4).

With the publication of *Basic Principles on Establishing a Regional Settlement Intermediary and Next Steps Forward* in May 2014, it was agreed that the CSD and real-time gross settlement (CSD-RTGS) linkages, which bilaterally connect domestic CSD and RTGS systems, would enable local bonds to be settled via delivery-versus-payment with central bank money to ensure the safety of settlement while being compliant with international standards and achieving cost efficiency. As CSIF members work toward realizing CSD-RTGS linkages, issues related to cross-border business continuity planning and cybersecurity have been identified as important elements in ensuring resiliency to unexpected or unforeseen events that could negatively affect the stability of such systems.

This report contains a set of basic common understandings on cross-border business continuity planning and cybersecurity frameworks, focusing on cross-border CSD–RTGS linkages. It discusses five key elements necessary to establish sound and resilient cross-border payment and settlement systems within the region: governance, compliance, relevance, understanding, and identification. Importantly, this set of common understandings may be reviewed and updated after the actual implementation of CSD-RTGS linkages among CSIF members.

Introduction

As part of efforts to promote cross-border investment in and settlement of local currency bonds within the region, the finance ministers and central bank governors of the Association of Southeast Asian Nations (ASEAN), the People's Republic of China, Japan, and the Republic of Korea (ASEAN+3) agreed to establish the Cross-Border Settlement Infrastructure Forum (CSIF) in May 2013, which included the possibility of creating a Regional Settlement Intermediary (RSI).

The Asian Development Bank, as Secretariat of CSIF since its inception, published *Basic Principles on Establishing a Regional Settlement Intermediary and Next Steps Forward* in May 2014, which offered recommendations on establishing the RSI. Based on the principles that were proposed, CSIF members, comprising the central banks and central securities depositories (CSDs) as real-time gross settlement (RTGS) system operators, agreed that the CSD-RTGS linkages, which bilaterally connect domestic CSD and RTGS systems, would be an achievable model for cross-border settlement infrastructure in both the short-term and medium-term. Subsequently, the roadmap on establishing RSI was published in 2015, comprising three implementation phases followed by an integration phase by 2020.

As CSIF members are working toward realizing CSD-RTGS linkages by 2020, CSIF members agreed that the issues of business continuity planning (BCP) and cybersecurity should be considered simultaneously to ensure the resilience of increasingly interconnected financial systems.

Due to the interconnectedness at both domestic and international levels of financial market infrastructures (FMIs), they must be safe, secure, and robust against natural disasters and human-led cybercrimes. From this perspective, proper BCP and a clear cyber resilience framework are crucial to prevent the FMIs from causing any adverse effect to the entire financial system, both at the domestic and international levels.

In this regard, CSIF members unanimously agreed at the 12th CSIF meeting held in Manila in July 2017 that a common understanding among FMI operators of cross-border BCP and cybersecurity should be included as part of the discussion on cross-border CSD-RTGS linkages. In particular, discussions should include issues relating to the finality of cross-border settlement and payment systems, as well as the identification of critical operations to ensure that financial systems in ASEAN+3 run smoothly.

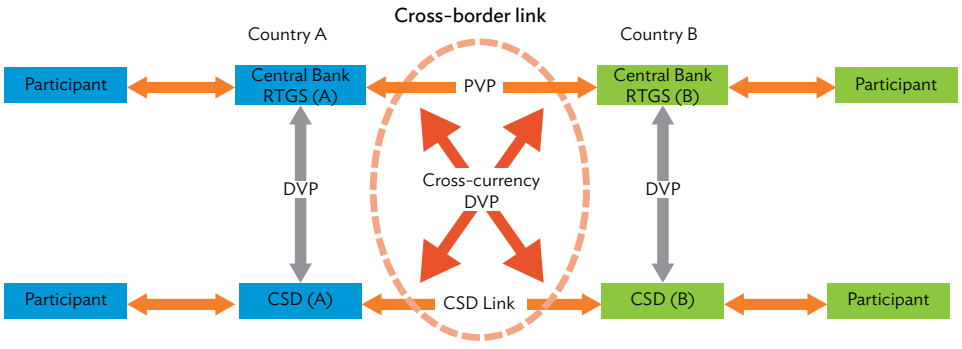
This paper aims to create a common understanding on BCP and cybersecurity in developing sound and resilient BCP and cybersecurity frameworks to facilitate the discussion on implementation of CSD-RTGS linkages in the region.

Cross-Border Central Securities Depository-Real-Time Gross Settlement Linkages

The Cross-Border Central Securities Depository-Real-Time Gross Settlement (CSD-RTGS) linkage for cross-currency delivery-versus-payment settlement was chosen as the first desktop study model by Cross-Border Settlement Infrastructure Forum (CSIF) members and regarded as the most suitable and achievable model for cross-border settlement infrastructure in both the short-term and medium-term.[1]

Under this model, a CSD in an economy will connect with the RTGS system of the central bank in another economy through a gateway (Figure 1). The connection allows for delivery-versus-payment settlement for cross-currency repo and settlement of foreign-currency-denominated bonds. This model facilitates settlement finality as the settlement is completed using central bank money. This is in line with the Committee on Payments and Market Infrastructures and the Board of the International Organization of Securities Commissions' (CPMI-IOSCO) Principles for Financial Market Infrastructure (PFMI) in the context of settlement finality (Principle 8) and money settlement (Principle 9). The settlement of securities takes place by book entry on the account of CSD participants, while the cash settlement takes place through the central bank's RTGS system.

Figure 1: Central Securities Depository-Real-Time Gross Settlement Linkage Model



CSD = central securities depository, DVP = delivery-versus-payment, PVP = payment-versus-payment, RTGS = real-time gross settlement.

Source: Asian Development Bank. 2014. *Basic Principles on Establishing a Regional Settlement Intermediary and Next Steps Forward*. Manila.

[1] The two other models are CSD-CSD linkage and RTGS-RTGS linkage. A CSD-CSD linkage connects an issuer CSD and investor CSD and aims to provide an access channel for investment in securities in the issuer CSD. An RTGS-RTGS linkage connects two RTGS systems in different economies and aims to achieve payment-versus-payment settlement for foreign exchange transactions.

This model is also in line with the *Basic Principles on Establishing a Regional Settlement Intermediary and Next Steps Forward* published by the Asian Development Bank, in consultation with CSIF members, in May 2014 (Figure 2). It allows new members to join when they are ready, thus the linkage can start from bilateral links, before expanding regionally. The linkage also promotes inclusiveness by allowing smaller participants, as members of a national CSD, to participate and benefit from regional integration.

Given the importance of sound and resilient linkages among regional CSD and RTGS operators, it is important that CSIF members maintain smooth operation of the critical business functions and resiliency of the systems to potential cyber risks that the financial market infrastructures (FMIs) may face.

Figure 2: Basic Principles on Establishing a Regional Settlement Intermediary and Next Steps Forward

Source: Asian Development Bank. 2014. *Basic Principles on Establishing a Regional Settlement Intermediary and Next Steps Forward.* Manila.

The Importance of Cross-Border Business Continuity Planning and Cybersecurity

Widespread natural disasters, increased geopolitical risks, and mounting cyber threats have heightened the priority of business continuity planning (BCP) efforts among policy makers and financial institutions. Large-scale cyberattacks, including data fraud and theft were highlighted by the World Economic Forum as the two biggest threats to global stability in terms of likelihood, while rising cyber-dependency was ranked as the second most significant driver shaping the global risk landscape over the next 10 years.[2] In Asia, NTT Security estimated that the two sectors that are targeted in a combined 78% of all cyberattacks are finance (46%) and manufacturing (32%).[3]

...hackers gaining access to customers' internet-based trading accounts with securities brokers, resulting in unauthorized trades totaling more than $110 million.

In Hong Kong, China, the number of cybersecurity incidents increased 25% in 2016 to reach 6,058 as reported by Hong Kong Productivity Council's Computer Emergency Response Team Coordination Centre. Additionally, the Hong Kong Securities and Futures Commission reported that for an 18-month period up to 31 March 2017, 12 licensed corporations reported 27 cybersecurity incidents, most of which involved hackers gaining access to customers' internet-based trading accounts with securities brokers, resulting in unauthorized trades totaling more than $110 million.[4]

Trigger events may differ from country to country, each of which has different response and recovery procedures as a result of different market structures, laws, rules, regulations, and levels of development. Most Cross-Border Settlement Infrastructure Forum (CSIF) members have put in place a well-designed BCP and cybersecurity framework within their respective institutions; and issued recommendations to their regulated entities such as financial institutions, and financial market infrastructures (FMIs). Most of the BCP guidelines that have been implemented are largely in line with the PFMI Principles, particularly in the context of operational risk (Principle 17).[5]

---

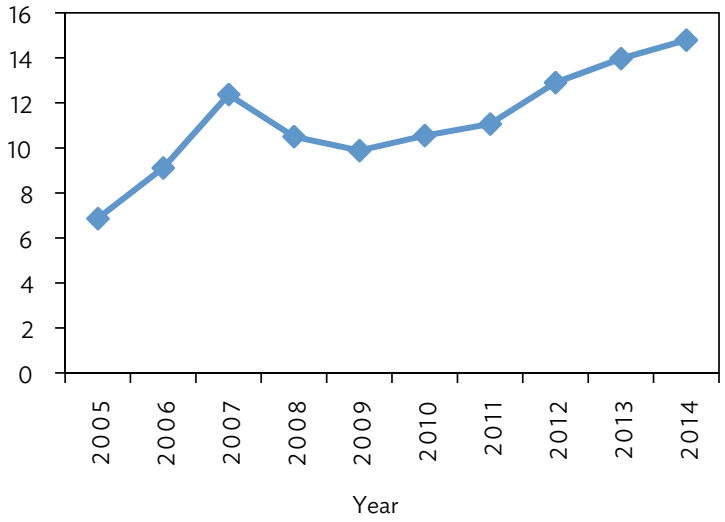
2 World Economic Forum. 2018. *The Global Risks Report*. Cologny.

3 NTT Security.2017. *Global Threat Intelligence Report*. Ismaning.

4 Securities and Futures Commission. 2017. *Consultation Paper on Proposals to Reduce and Mitigate Hacking Risks Associated with Internet Trading*. Hong Kong.

5 Principle 17 (operational risk) states that an FMI should identify the plausible sources of operational risk, both internal and external, and mitigate their impact through the use of appropriate systems, policies, procedures, and controls. Systems should be designed to ensure a high degree of security and operational reliability and should have adequate, scalable capacity. Business continuity management should aim for timely recovery of operations and fulfillment of the FMI's obligations, including in the event of a wide-scale or major disruption.

Figure 3: Portfolio Share (%) in Association of Southeast Asian Nations, the People's Republic of China, Japan, and the Republic of Korea (ASEAN+3)



Note: Portfolio share is the percentage of intraregional portfolio assets to total portfolio assets held by countries in the region. A higher share indicates a higher degree of integration.

Source: Asia Regional Integration Center.

As financial markets become more integrated (as evidenced by increased intraregional investment), it is necessary to have a mutual understanding on the scenarios, practices, and procedures among ASEAN+3's FMIs to maintain the stability and resiliency of regional financial markets. As cross-border investment increases (Figure 3), it is important to ascertain the finality of cross-border transactions as the settlement and payment risks triggered by failed trades or technical glitches in the IT infrastructure of an FMI can quickly spread across boundaries and seriously impact securities settlement in other jurisdictions.

Ideally, the finality of transactions should be ascertained within the day of disruption or else counterparties should be able to unwind the transaction to minimize the potential unfavorable impact to financial markets. It is important that relevant clearing and settlement, as well as payment systems, are resilient to natural disasters, cyberattacks, and other means of disruptions.

Given the importance of BCP and cybersecurity frameworks, CSIF members agreed to develop a common understanding on cross-border BCP and cybersecurity focusing on cross-border CSD-RTGS linkages to ensure the finality and irrevocability of transactions. These common understandings are based on existing methodologies and procedures that have been implemented and accepted by individual FMI operators based on internationally accepted principles to the extent possible.

Common Understanding on Cross-Border Business Continuity Planning and Cybersecurity Frameworks

In a domestic market, securities are usually settled via a book-entry system on the securities account of a central securities depository (CSD) participant, while cash settlement occurs simultaneously through the real-time gross settlement (RTGS) system operated by the central bank. The business continuity planning (BCP) and cybersecurity frameworks of these systems are often subject to oversight by regulatory authorities at the national level, based on internationally accepted guidelines and practices to ensure proper implementation and compliance.

However, the issues become more complex for a cross-border transaction as it involves various domestic and international financial market infrastructures as well as differing legal frameworks among the jurisdictions involved. To ensure sound and resilient cross-border linkages of payment and settlement systems within the region, CSIF members agreed on the following:

1. Governance. Cross-border BCP and cybersecurity frameworks should be driven, supported, and understood by the board and senior management of financial market infrastructure (FMIs). According to the World Economic Forum, cyber resilience is more a matter of strategy and culture than tactics. Being resilient requires those at the highest levels of a company, organization, or government to recognize the importance of avoiding and proactively mitigating risks. The Bank for International Settlements also suggested that an organization's board and senior management are responsible for managing its business continuity effectively and for developing and endorsing appropriate policies to promote resilience to and continuity in the event of operational disruption. They are also ultimately responsible for setting the cyber-resilience framework and ensuring that cyber risks are effectively managed. The frameworks should specify a clear command line and identify an accountable officer who understands the business process, particularly those related to critical business operations so that strategic decision can be made.

2. Compliance. Cross-border BCP and cybersecurity frameworks should comply with guidelines issued by domestic regulators as well as internationally recognized best practices. The Bank for International Settlement's Committee on Payments and Market Infrastructures and the board of International Organization of Securities Commissions (IOSCO) jointly issued guidance on cyber resilience for international market infrastructures in 2016 to help FMIs enhance their cyber resilience and to provide supplemental guidance for the Principles for Financial Market Infrastructure (PFMI) of Committee on Payments and Market Infrastructures (CPMI)-IOSCO, primarily in the context of governance (Principle 2), the framework for the comprehensive management of risks (Principle 3), settlement finality (Principle 8), operational risk (Principle 17),

and FMI links (Principle 20).[6] High-level principles for business continuity were also published by the Basel Committee on Banking Supervision in 2006. Furthermore, the development of cross-border BCP and cybersecurity frameworks should be consistent with discussions under other regional fora, particularly the ASEAN's Working Committee on Payment and Settlement Systems. Compliance with international standards and regional policy dialogues will facilitate multilateral linkages of CSD-RTGS systems in the long-term.

3. Relevance. Cross-border BCP and cybersecurity frameworks should accommodate different trigger events such as terrorism, natural disasters, disease outbreak, malware, and ransomware. Since the severity and likelihood of each event happening varies across countries, the details of individual frameworks do not necessarily need to be the same. The frameworks and triggering scenarios should also be developed with a sufficient level of granularity to accommodate the different levels of crisis. Critical business flows should be discussed at the working level and be reviewed from time to time to accommodate the changing environment, technological development, and emerging types of cyber threats.

4. Understanding. The basic principles in establishing a regional Regional Settlement Intermediary suggest that the bilateral linkage of a CSD-RTGS system is achievable in the short-term and medium-term; thus, cross-border BCP and cybersecurity frameworks should also be established on a bilateral basis. It should be included as an important element of the entire framework for FMIs such that critical cross-border services, particularly the finality of the settlement among the connected FMIs, will remain uninterrupted, or if interrupted, can be recovered within a mutually agreed and reasonable time period. Therefore, the BCP and cybersecurity frameworks of both FMIs should be shared and thoroughly understood among connected FMIs. This would allow cross-border communication among FMIs to be carried out more efficiently through relevant accountable officers. Besides, having a common understanding of one another's framework would allow parties involved to make an informed decision in adjusting or adapting procedures given the uniqueness and severity of the event.

5. Identification. Cross-border BCP and cybersecurity frameworks should cover the critical business operations of FMIs, particularly securities settlement and relevant payment systems. The critical operation functions should be jointly identified by relevant FMIs such that contingency business operations can be properly carried out in the event of a disruption. More importantly, the frameworks should ascertain the finality of cross-border transactions on the day of disruption. Preferably, the critical business operations should be resumed as soon as practicable or within a mutually agreed timeframe. Otherwise, counterparties should be able to unwind the transaction to minimize the potential negative impact on financial markets.

[6] CPMI-IOSCO. 2016. *Guidance on Cyber Resilience for Financial Market Infrastructures.* Madrid.

Next Steps

The Cross-Border Settlement Infrastructure Forum (CSIF) will continue to serve as a place to share information on various developments in cross-border securities settlement infrastructure within the Association of Southeast Asian Nations, the People's Republic of China, Japan, and the Republic of Korea (ASEAN+3) region. To support the expansion of bilateral central securities depository-real-time gross settlement (CSD-RTGS) linkages among ASEAN+3, the CSIF should identify and prioritize possible implementation challenges, including legal barriers and market-practice-related impediments. If necessary, the CSIF could conduct a stock taking exercise on identified challenges.

It is expected that the Common Understanding on Cross-Border (BCP) and Cybersecurity will create awareness among CSIF members with respect to cross-border linkages of CSD-RTGS systems in the region. The draft may be reviewed and updated after actual implementation of such CSD-RTGS linkages among CSIF members.

Common Understanding on Cross-Border Business Continuity Planning and Cybersecurity

Cross-Border Settlement Infrastructure Forum

This publication developed by the Cross-Border Settlement Infrastructure Forum, composed of the central banks and central securities depositories of the Association of Southeast Asian Nations and the People's Republic of China, Japan, and the Republic of Korea—collectively known as ASEAN+3—is an important discussion topic as members work toward realizing the establishment of central securities depository and real-time gross settlement linkages in the region. This report sets out a broad, common understanding on the important elements of cross-border business continuity planning and cybersecurity, particularly on issues relating to the finality of cross-border settlement and payment systems. As Secretariat of the Cross-Border Settlement Infrastructure Forum, the Asian Development Bank supports this initiative.

About the Asian Development Bank

ADB's vision is an Asia and Pacific region free of poverty. Its mission is to help its developing member countries reduce poverty and improve the quality of life of their people. Despite the region's many successes, it remains home to a large share of the world's poor. ADB is committed to reducing poverty through inclusive economic growth, environmentally sustainable growth, and regional integration.

Based in Manila, ADB is owned by 67 members, including 48 from the region. Its main instruments for helping its developing member countries are policy dialogue, loans, equity investments, guarantees, grants, and technical assistance.

ADB

ASIAN DEVELOPMENT BANK
6 ADB Avenue, Mandaluyong City
1550 Metro Manila, Philippines
www.adb.org