INTERNATIONAL MONETARY FUND

Operational Resilience in Digital Payments

Experiences and Issues

Tanai Khiaonarong, Harry Leinonen, and Ryan Rizaldy

WP/21/288

2021
DEC

WORKING PAPER

 WP/21/288

IMF Working Paper
Monetary and Capital Markets Department

Operational Resilience in Digital Payments: Experiences and Issues

Prepared by Tanai Khiaonarong, Harry Leinonen, and Ryan Rizaldy*

Authorized for distribution by Tommaso Mancini-Griffoli
December 2021

ABSTRACT: Major operational incidents in payment systems suggest the need to improve their resiliency. Meanwhile, as payment infrastructures become more digitalized, integrated, and interdependent, they require an even higher degree of resilience. Moreover, risks that could trigger major disruptions have become more acute given the rise in power outages, cyber incidents, and natural disasters. International experiences suggest the need to strengthen reliability objectives, redundancies, assessment of critical service providers, endpoint security, and alternative arrangements.

JEL Classification Numbers:	E42 E58 E59 M15
Keywords:	Operational resilience, payment systems, risks, disasters, business continuity
Author's E-Mail Address:	tkhiaonarong@imf.org; harry.leinonen@gmail.com; rrizaldy@imf.org

* The authors would like to thank Rachel van Elkan, Julia Faltermeier, Diep Ferris, Emran Islam, Arif Ismail, Andy Jobst, Majid Malaika, Marcello Miccoli, Jan Nolte, and Sali Osman for their inputs and comments. Erica Sandoval provided editorial assistance.

WORKING PAPERS

Operational Resilience in Digital Payments

Experiences and Issues

Prepared by Tanai Khiaonarong, Harry Leinonen, and Ryan Rizaldy

Contents

I. Introduction

> *"We'd always thought that if you wanted to cripple the U.S. economy, you'd take out the payment systems. Banks would be forced to fall back on inefficient physical transfers of money"*
>
> Alan Greenspan, *The Age of Turbulence*

While the events of September 11, 2001 was a wake-up call for the operational resilience of critical nodes and financial markets two decades ago, it is even more relevant today.[1] The rise of new digital payment services and associated operational risks; tighter interdependencies of systems, institutions and operating environments; increased global trade and electronic commerce, reoccurrence of operational incidents; and evolving risks, have reinforced the need to understand, regulate, and re-think, the design of resilient payment systems.

This paper attempts to draw lessons from recent operational incidents and suggest ways in which operational risk management frameworks could be strengthened given evolving payment systems, user expectations, technologies, and country circumstances. The work is motivated by ongoing developments as follows.

First, greater digitalization is transforming the payments landscape and has increased operational risks.[2] Electronic payments have become the major method for making consumer, business, and government payments in many societies. User expectations for faster payments with round-the-clock availability would become the future norm. There are new technologies—application programming interfaces, big data analytics, biometric technology, cloud computing, contactless technologies, digital identification, distributed ledger technology, and the Internet of things—implemented within payment infrastructures. There are new products and service offerings—instant payments, central bank digital currencies (CBDC), and stablecoins. And there are new access points for payment initiation—electronic wallets, open banking, and super apps. Consequently, this has spurred new business models and service offerings (CPMI and World Bank, 2020).

Second, interdependencies are arising with the increased reliance on third-party service providers, critical infrastructures, and cross-border links. For example, the number and duration of major power outages have increased. Financial market infrastructures (FMIs) and payment service providers (PSPs) have benefitted from outsourcing and offshoring arrangements to address cost and specialization needs. However, this also comes with operational risks and resiliency challenges to ensure the continuity of critical services in the event that a third-party service provider faces an outage or business failure. Electronic payments are completely dependent on electricity, telecommunications, and computer hardware/software. Commerce and customer services would also become dependent on electronic payments and its continued availability, especially to meet just-in-time demand. Interdependencies also extend at the global level.

[1] The event caused major power outages and much of the telecommunications infrastructure was unavailable for several days. The destruction disrupted interbank payments. Payment processing was delayed at many banks, closing times were pushed back, and the volume of settlement "fails" increased. See Bech and Garratt (2012), Lacker (2004), and Fleming and Garbade (2002) for a further analysis on the impact of events of September 11th on payment systems.

[2] This paper focuses on digital and electronic payments, which refers to all types of non-paper-based payment instruments initiated electronically by users and cleared among payment service providers using electronic payment systems. The scope is applicable to emerging service offerings such as mobile payments, central bank digital currencies, crypto-currencies, and stablecoin arrangements in addition to more traditional electronic payment instruments such as card payments, credit transfers, and direct debits.

Third, recent incidents of major retail and systemically important payment systems (SIPS) have raised concerns on operational resilience and preparedness. While prolonged outages of retail payment systems could lead to a loss of public confidence, similar incidents in the case of wholesale payment systems could disrupt monetary operations, settlement of capital market transactions, and other high-value or urgent payments. Modernization efforts, such as the renewal of real-time gross settlement (RTGS) systems, have included resiliency enhancements in addition to supporting competition and innovation (Cleland, 2021).

And fourth, evolving risks such as cyber-attacks, natural disasters, and pandemics have called for greater oversight expectations for operators to continuously improve operational resilience. The number of cyber incidents relating to financial institutions has increased substantially. Cyber criminals and terrorists have become more sophisticated and better trained in attacking payment systems and digital infrastructures in general. The consequential impact of natural catastrophes hitting digital infrastructures and associated risks would also grow.

The paper is organized as follows. Section II defines operational resilience, examines risk scenarios, and reviews existing international principles relating to operational resilience. Section III shares observations from international experiences. Section IV explores operational and developmental issues to strengthen the operational resilience of existing and future payment systems. Section V concludes and explores future research topics

II. Operational Resilience

This section defines operational resilience, examines risk scenarios, and reviews existing international principles relating to operational resilience.

A. Definition

Operational resilience is defined as the ability of a payment system and its service providers to deliver critical operations in disaster situations and extreme circumstances.[3] The Principles for Financial Market Infrastructures (PFMI) provides guidance in relation to operational risk and business continuity planning, stating:

"*An FMI should have a business continuity plan that addresses events posing a significant risk of disrupting operations, including events that could cause a wide-scale or major disruption. The plan should incorporate the use of a secondary site and should be designed to ensure that critical information technology systems can resume operations within two hours following disruptive events. The plan should be designed to enable the FMI to complete settlement by the end of the day of the disruption, even in case of extreme circumstances. The FMI should regularly test these arrangements*."

[3] This definition is used for the purpose of this paper and is also relevant for other types of payment service providers and FMIs. The latter includes securities settlement systems, central securities depositories, central counterparties, and trade repositories. Tiernan et al., (2019) emphasizes three key elements, including (i) the ability of a system to remain stable in the face of external perturbations and stresses; (ii) recover following a major disruption; and (iii) adapt to new circumstances. Therefore, resiliency does not merely deal with disaster recovery, but most importantly, high availability.

Additionally, the PFMI states that reliability and resilience are oversight expectations required for FMI critical service providers (such as information technology and messaging providers). Redundancy is expected for the primary and secondary sites of a payment system. Each site should have robust resilience based on the duplication of software and hardware. Arrangements also need to replicate data between the various sites and should be consistent with chosen recovery-point objectives. Other considerations include distinct risk profiles between the primary and secondary sites, single point of failure mitigation, and alternative arrangements (for example, manual paper-based procedures) to enable the processing of time-critical transactions in extreme circumstances.

International experiences suggest four sound practices: (i) identifying clearing and settlement activities in support of critical financial markets; (ii) determining appropriate recovery and resumption objectives for clearing and settlement activities in support of critical markets; (iii) maintaining sufficient geographically dispersed resources to meet recovery and resumption objectives; and (iv) routinely using and testing recovery and resumption arrangements.[4]

Operational resilience has been viewed as distinct from business continuity management and disaster recovery plans. It is the "*ability of FMIs and the sector as a whole to prevent, respond to, recover and learn from operational disruptions*" (BoE, 2021a), and requires: (i) developing an operational resilience framework, which is subject to governance arrangements for audit assessments; (ii) identifying important services, operational activities, and associated operational risks; (iii) setting the impact tolerance[5] for each service; (iv) mapping interdependencies; and (v) testing, monitoring, and reporting. [6]

Further efforts have been made to harmonize regulatory approaches to operational resilience in the financial sector. For illustration, the European Commission's proposed Digital Operational Resilience Act (DORA) would seek to harmonize digital operational resilience rules for financial organizations in the EU.[7] DORA would apply to financial entities (such as credit and payment institutions, electronic money institutions, and crypto-asset service providers) and ICT third-party service providers (such as providers of cloud computing services, software, data analytics and data centers).

While the need to address operational resilience is commonly recognized, international experiences have identified serious issues of concern. This includes observance of the two-hour recovery time objective (2h-RTO) benchmark for FMIs, including in the event of a wide-scale or major disruption (CPMI-IOSCO, 2021). Also, international practices suggest that operational reliability objectives (OROs) could differ from system availability,

[4] See Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System (2003). These practices focused on critical financial markets, core clearing and settlement organizations, and firms that play significant roles in critical financial markets, due to their potential impact on systemic risks. Although the practices did not directly address retail financial services, the practices are largely relevant for retail payment systems and payment service providers that have grown in importance in some jurisdictions.

[5] Impact tolerance refers to the maximum tolerable level of disruption for an important business service, whereby further disruption could significantly threaten the transfer of payments or the safety and efficiency of the payment system (BoE, 2021). Of relevance were findings from earlier cyber simulation exercises that identified opportunities to improve firm coordination, disparity in risk tolerance for suspending services, constraints in restoring data and service recovery, and the importance of communication practices for incident management (BoE, 2019).

[6] See BoE (2021). The Policy Statement and Supervisory Statement on operational resilience for recognized payment system operators and specified service providers targets importance business services where operational activities could involve tokenization, settlement instructions, debit payments, credit payments, interbank payments, or cash withdrawals.

[7] See European Commission (2020). Public consultations concluded on 12 April 2021.

recovery time, or other objectives. While quantitative targets are commonly used, qualitative objectives are also practiced. Guidance to ensure resiliency against cyber threats or attacks were also issued (CPMI-IOSCO, 2016).

From a technical standpoint, the objective to improving operational resilience is further complicated by several factors, including: technical and organizational complexity; dependence on single software versions; dependence on external infrastructures; vulnerability of information security solutions; geographical, jurisdictional, and time-zone issues; and insufficient incentives for resilience (Appendix 1).

B. Wide-Scale or Major Disruption Scenarios

The PFMI also defines a wide-scale or major disruption as events that can pose significant risks to FMIs. Such disruptions could be defined as: "an event that causes a severe disruption or destruction of transportation, telecommunications, power, or other critical infrastructure components across a metropolitan or other geographic area and the adjacent communities that are economically integrated with it; or that results in a wide-scale evacuation or inaccessibility of the population within normal commuting range of the disruption's origin."[8] Operational disruption is an unavoidable risk for organizations and reflects the frequency of unexpected events that could interrupt a firm's smooth flow of operations (Essuman, et al. 2020).

While operational risk has been generally understood, assessed, and managed in many payment systems, the aim to maintain operational resilience faces several challenges. This includes the rising demand for around-the-clock and real-time payments, emerging technologies, increasing interdependencies, and evolving risks.

Plausible sources of operational risk could be internal and external and could differ in scale and time. Such risks are a technological shock such as a significant loss of operational capability arises from the loss or malfunction of physical capital or staff (Lacker, 2004). Figure 1 illustrates 10 risk scenarios (noted in brackets, hereafter). *Internal sources* typically include: (1) inadequate arrangements (risk identification and understanding, human errors, controls and procedures, personnel screening, management); (2) internal sabotage; and (3) workplace violence (active shooter).

External sources could come from: (4) civil disturbances (political protest, social unrest); (5) failure of critical service provides or utilities; (6) pandemics; (7) terrorism and warfare (advanced persistent threat, bombings, biological and chemical warfare); (8) cyber-attacks and cyber-warfare; (9) natural disasters (bushfires, earthquakes, floods, haze, hurricanes, tornadoes, winter storms); and (10) mega disasters.

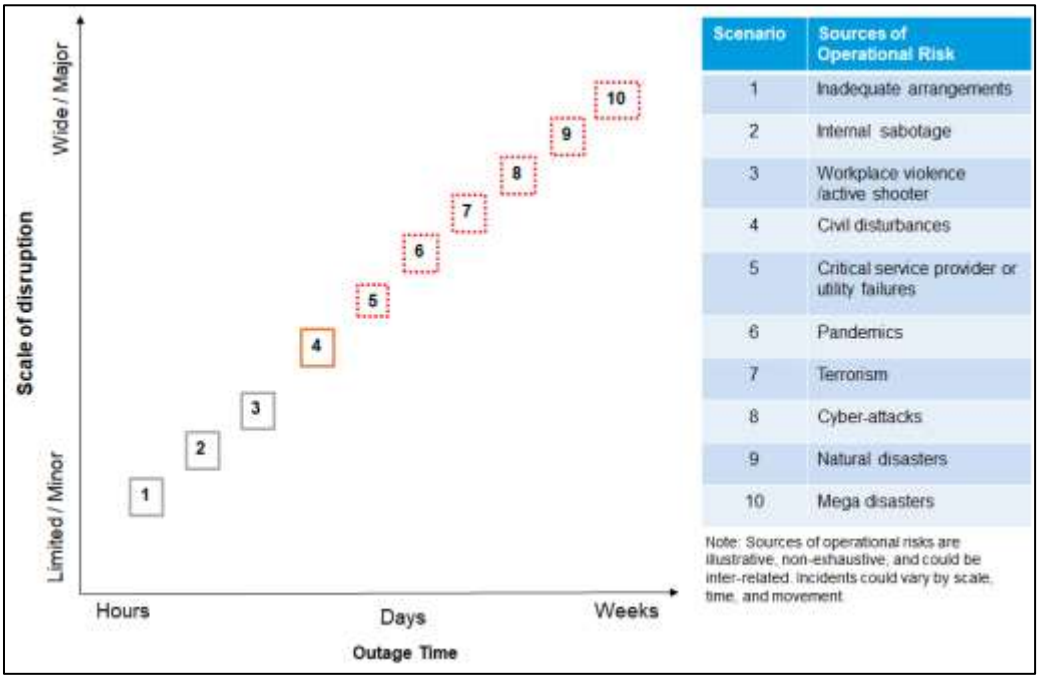
Operational risks, if materialized, could compromise financial stability and public confidence. This is relevant for SIPS and retail payment systems or payment services that are widely used. For example, the physical destruction of centralized infrastructure with ineffective business continuity plans (BCP) could affect monetary operations, settlement of money and capital market transaction, and interbank payments. Digital payments are dependent on the functioning of service providers' customer account systems.

A cyber-attack on a systemically important bank could disrupt its outgoing and incoming payments flows and create intraday liquidity risks to other participants in the payment system and to their customers. As such, international efforts have been made to secure the core and periphery of payment ecosystems from cyber-attacks

[8] See Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System.

(CPMI-IOSCO, 2016; CPMI, 2019). For retail payment systems, a prolonged outage of a major payment card network could make debit or credit card payments at electronic funds transfer at point of sales terminals impossible.

Figure 1. Risk Scenarios—Scale of Disruption and Outage Time



Scenario	Sources of Operational Risk
1	Inadequate arrangements
2	Internal sabotage
3	Workplace violence /active shooter
4	Civil disturbances
5	Critical service provider or utility failures
6	Pandemics
7	Terrorism
8	Cyber-attacks
9	Natural disasters
10	Mega disasters

Note: Sources of operational risks are illustrative, non-exhaustive, and could be inter-related. Incidents could vary by scale, time, and movement.

Source: IMF staff.

Furthermore, efforts to maintain operational resilience against sophisticated, coordinated, or simultaneous incidents also pose new challenges.[9] For example, a coordinated terrorist attack on the primary and secondary sites of a payment system that lack distinct risk profiles could potentially cripple it even when inter-site switchovers are activated (or may necessitate considerations for a third site). Consequently, this could unnecessarily prolong the outage. This applies to both domestic and cross-border payment system and arrangements.

As operational incidents increase in complexity in the future, this would require cross-sectoral and/or cross-border crisis management arrangements, involving multiple authorities and stakeholders. Individual incidents could vary considerably in terms of their outage time and impact on the payment system and overall economy. Six plausible risk scenarios that could cause wide-scale or major disruptions are discussed below.[10]

[9] Hybrid threat has been a term used for this context and is considered relevant for the critical points in the financial sector. See European Commission (2017).

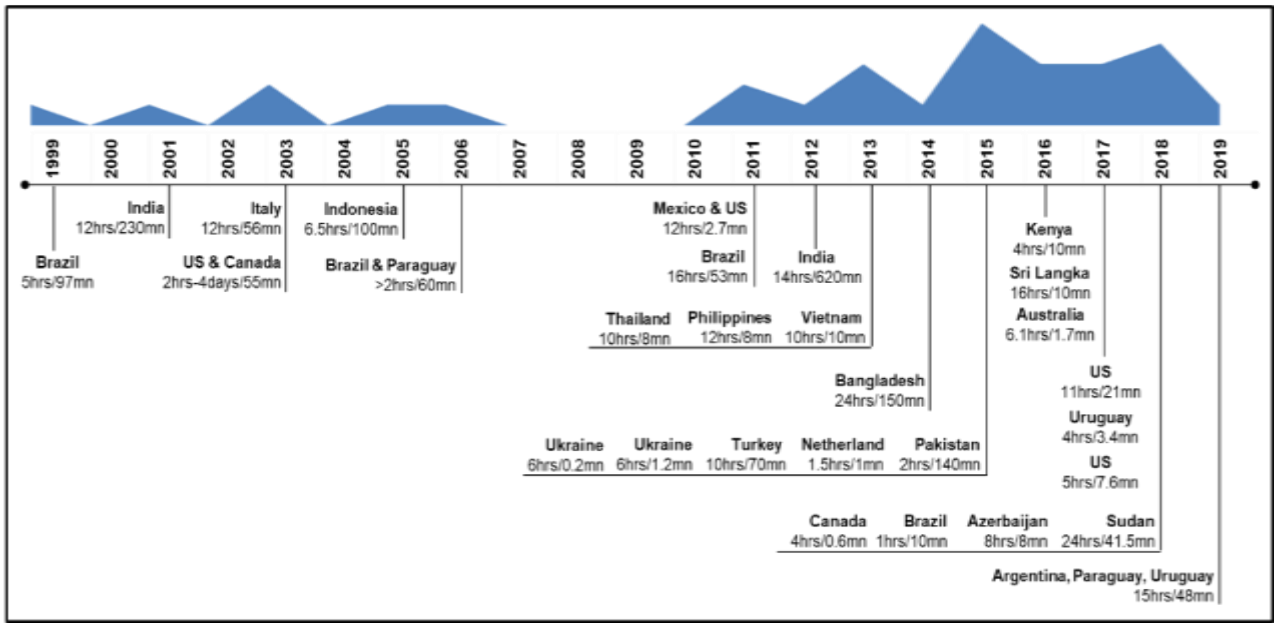
[10] This is a non-exhaustive list of possible scenarios. Geoeconomic risk is also another emerging area, which involves the weaponization of economic networks such as payment systems and messaging services (Fjader et al., 2021).

Critical service provider or utility failures

This scenario could include the outage of the telecommunications network, messaging provider, or common cloud service provider used by the financial sector disrupting payment submissions by banks and settlement by the central bank. This has become an increasing threat to financial stability if there is high concentration, tight interdependencies with financial institutions and FMIs, and other inter-relationships with other entities from a supply chain perspective.

Power outages, which some countries have experienced for several hours or days, could also disrupt economic activity and the delivery of critical services in the financial sector (Figure 2). Electronic payments require noninterrupted power supply throughout the entire processing chain end-to-end. Power outages could stem from underinvestment in public and private utilities or result from other external sources such as from a natural disaster.

Figure 2. Major Power Outages, 1999-2019



Source: Owens et. al., (2019); Alhelou et. al., (2019).

Pandemics

This scenario could involve increased staff absenteeism or loss of key personnel of a SIPS operator or outsourcing firm that processes the data of a systemically important bank or payment system. Pandemics could also affect the availability of critical service providers and infrastructures such as governments ordering the shutdown of internet services. Given their economic and financial impact, a few countries have analyzed preparedness levels through pandemic exercises (FSA et al., 2008; U.S. Department of the Treasury, 2008; IMF, 2006). Best practices applied by FMIs during the COVID-19 pandemic has also involved setting up pandemic management teams, and developing and implementing pandemic management plans (ECB, 2021a).

Terrorism

This scenario could unfold as physical attacks targeting central bank RTGS systems, clearing houses, or cross-border and multi-currency payment systems. Transnational terrorism and geopolitical tensions could motivate such disruptions. For example, this could include unilateral sanctions imposed on identified financial institutions or individuals of one country by another for violating sanction laws. Consequently, this could suspend such entities or individuals from accessing payment systems or messaging services.

Cyber-attacks and cyber-warfare

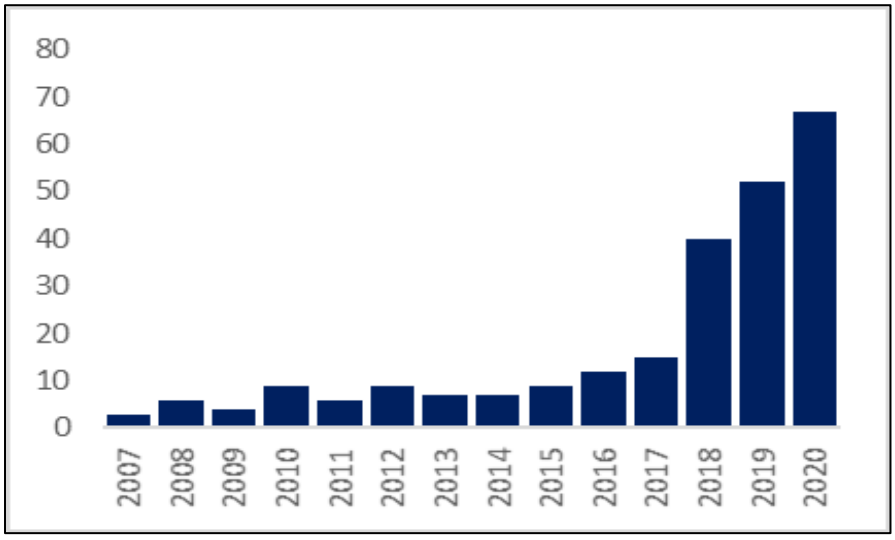
This scenario could include coordinated attacks on critical national information and telecommunication infrastructures, creating major power outages and hitting critical payment system. The financial sector is estimated to be three times more at risk of cyber-attacks than any other sector (European Parliament, 2017). Cyber risk is one of the sources of systemic risk to the global financial sector (ESRB, 2020). Many national financial systems are unready to manage attacks, while international co-ordination is still weak (Adelmann et.al., 2020).

Rapid digitization of the global economy is also leading to a dramatic increase in the number of cyber security incidents. Cyberattacks have become increasingly seen as a threat to financial stability as financial institutions become ever more reliant on digital services (e.g. cloud and APIs.) A survey by the Carnegie Endowment for International Peace identified at least 200 cyber incidents targeting financial institutions since 2007, which has been on a rising trend (Figure 3).

Industry surveys (by Carbon Black) also found that 46 percent of organizations were typically unable to contain a cyber threat in less than one hour while 23 percent of organizations that experienced more than three data compromises needed at least 12 hours to contain a threat.

Cyber risk is fundamentally different from other sources of operational risk whereby a combination of factors makes cyber risk so potent (ESRB, 2020). For example, financial services firms have experienced an increase in cyber-attacks following the rapid adoption of remote access during the COVID-19 pandemic (IBM, 2020; MAS, 2020; FSB, 2020b; Aldasoro et.al, 2020). Many cyber-breaches were also intertwined with terrorism. Such overlapping disruptions could cause a domino effect that intensifies—and further complicates predictions of—the economic chaos it creates (IBM, 2020).

Figure 3. Cyber Incidents Involving Financial Institutions, 2007–2020



Notes: Data on cyber incidents was obtained from the Carnegie Endowment for International Peace as of May 2021.

Source: IMF staff.

Natural disasters

This scenario could involve hurricane or earthquake damages to the primary and secondary sites of a payment system and/or mobile network operator in small states or developing countries vulnerable to large natural disasters (IMF, 2019a; IMF, 2016a; Cantelmo et al., 2019). Natural disasters could disrupt or damage critical infrastructure resulting in a lack of electricity and network connectivity and thus limiting the usefulness of electronic means of payment. Large natural disasters causing significant damage can substantially setback output growth (IMF, 2019a). Climate change and its multiplying catastrophes —drought, floods, storms— would make the risk hard to manage and pernicious as it will raise the uncertainty over their timing and magnitude of disaster (FSB, 2020a). Such catastrophes could often cause damages to physical infrastructures such as payment systems which facilitate economic and financial activities.

Mega disasters

This scenario could involve high impact but low probability events that are largely complex and have global implications. For example, the Great East Japan Earthquake was the first disaster ever recorded that included an earthquake, a tsunami, a nuclear power plant accident, a power supply failure, and a large- scale disruption of supply chains (Ranghieri and Ishiwatari, 2014). Such mega disasters emphasized the need for payment and settlement systems and financial institutions to review the severity and scope of scenarios used in designing business continuity arrangements to cope with potential stress events sufficiently, and their co-existence with other social infrastructure such as transportation, water, sewage, electricity, gas, and telecommunication (Bank of Japan, 2011; Wakatabe, 2019).

Other mega disaster scenarios could include nuclear incidents that spread contamination across wide geographical areas and compromise personnel safety and physical security. BCPs could be ineffective if the primary and secondary sites of payment processing facilities lack distinct risk profiles (in close proximity) or

sufficient power supplies. Another plausible scenario could involve hybrid attacks, which encompasses a range of different tactics and scenarios that combine together in a crystallized and coordinated fashion to cause significant disruption such as nuclear incidents coordinated through cyber-attacks.

C. International Principles and Assessments

The CPSS-IOSCO PFMI provides a general framework to assess operational risk in payment systems as mentioned earlier (CPSS-IOSCO, 2012a). For operational risk, there are seven key considerations which are further guided by specific questions relevant for the assessment of operational resilience (Appendix 2). Assessments of operational resilience could be guided through identification of any gaps, shortcoming, or issues of concerns relating to OROs, BCPs, and associated risks from key participants, other FMIs, and service and utility providers.

The Basel Committee on Banking Supervision (BCBS) Principles for Operational Resilience provides a complementary approach with an explicit, conceptual, pragmatic, and principles-based approach that helps analyze banks' critical functions associated with payments, clearing and settlement (BCBS, 2021).[11] In practice, some banks serve as settlement banks, custodian banks, correspondent banks, and major participants in payment systems. Moreover, the principles are relevant for the analysis of operational resilience of PSPs that could perform similar activities to banks, and FMI critical service providers. The BCBS Principles for Operational Resilience includes seven principles and considerations (Appendix 2).

Operational risk in payment systems is generally covered in the detailed assessment of SIPS in financial sector assessment programs led by the IMF and World Bank.[12] Such detailed assessments have benchmarked actual practices against the applicable principles of the PFMI since 2012, and its predecessor the Core Principles for SIPS of 2001. IMF assessments have also involved in-depth analyses of operational risks and resilience in the payment system and cyber security risk supervision and oversight.[13] This follows the analysis of outsourcing arrangements and other broader issues in the financial infrastructure (Norges Bank, 2021; Watne, 2012; Solheim and Strømme, 2004).

An important aspect of assessments is the mapping of interconnections and interdependencies given their implications for financial stability (Figure 4). Interdependencies exist at three levels—institutions (e.g. central bank, banks, firms), systems (e.g. payment system, securities settlement systems), and environments (e.g. third-party service providers, critical infrastructures). As noted earlier, such interdependencies among key participants, other FMIs and service and utility providers could serve as transmission channels for risks.[14] Furthermore, such mapping could identify potential concentration risks or single points of failure.

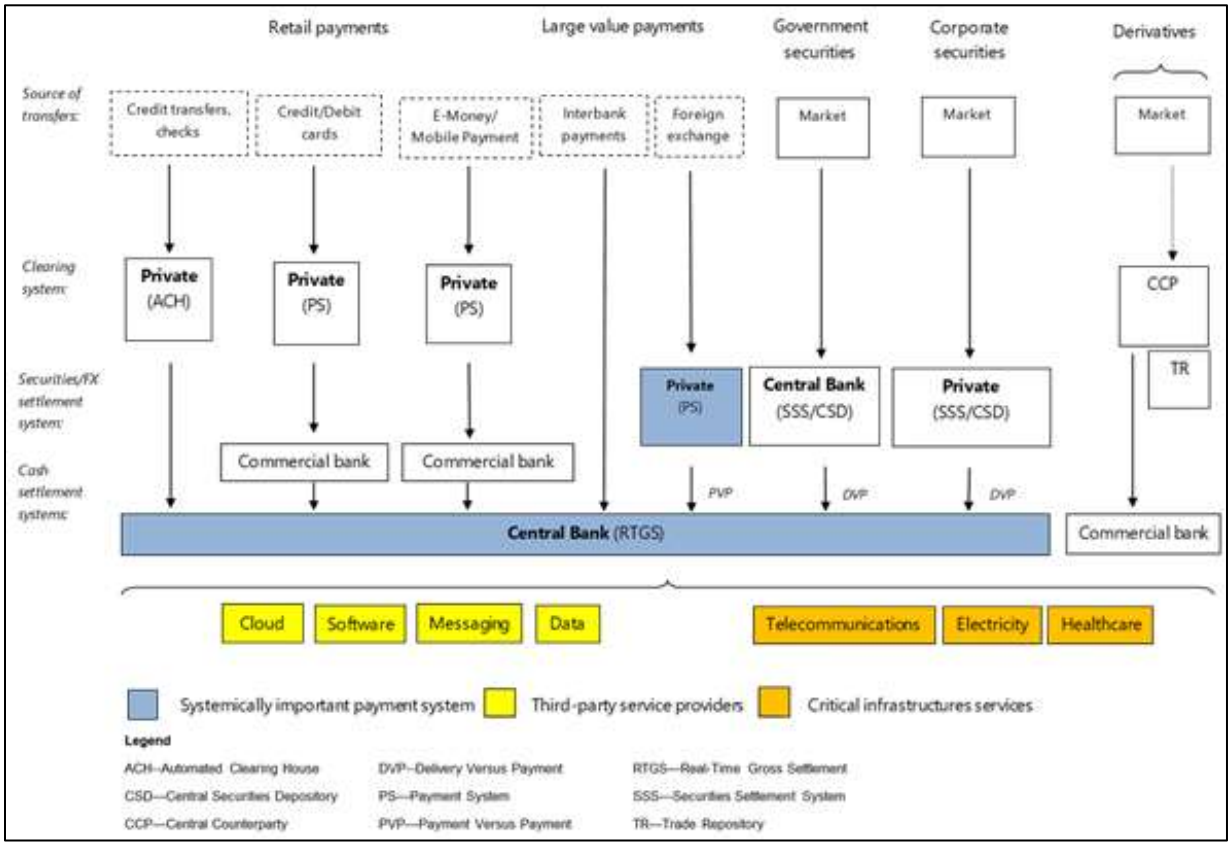
[11] See FSB (2013). Critical functions are defined as "activities performed for third parties where failure would lead to the disruption of services that are vital for the functioning of the real economy and for financial stability due to the banking group's size or market share, external and internal interconnectedness, complexity and cross-border activities."

[12] For example, see the detailed assessment of the RTGS systems for Singapore (IMF, 2019b), Bosnia and Herzegovina (IMF, 2015a), and the Kingdom of Bahrain (IMF, 2016b).

[13] See assessment reports for Norway (IMF 2020; IMF 2015b).

[14] For example, Euroclear's settlement outage in September 2020, which was caused by an issue with messaging software, delayed the Bank of England's regular gilt auctions (Source: Centralbanking.com).

Figure 1. Mapping of Interdependencies for Payment and Market Infrastructures



Note: This mapping is provided for illustrative purposes as the actual landscape for payments and FMI vary across jurisdictions and could include links with foreign entities.

Source: Authors.

Digitalization in the payments landscape has created further challenges in strengthening their resilience. Users of electronic payment services expect speed, rapid delivery times, and 24/7/365 service level availability. Therefore, this would require real-time (or near real-time) and uninterrupted payments processing. Digitalization is also marked with more complex business models. Organizations have multiple outsourcing partners, deeper interconnections, integration with domestic and overseas service providers, and higher dependency on utilities (e.g. electricity, telecommunications). In addition, cyber risk and cyber-terrorism have reached new dimensions and would present further challenges for large and small value payments.

As the public becomes increasingly reliant on technology as part of their daily activities, authorities are also being expected to ensure public confidence. Consequently, this would require the appropriate anticipation and seamless response times from payment service providers against any disruptions. The current redundancy arrangements that include primary and secondary sites-type of back-up systems appear to be inadequate to ensure resiliency in a real-time uninterrupted payment system. This is illustrated in the following section.

III. International Experiences

Are existing electronic payment systems resilient? A review of international experiences suggests otherwise as operational incidents occurred in critical service providers, payments and currency services, and even in SIPS (Appendix 3). These are high-level observations and are not a formal assessment of any payment system against the PFMI.

For example, there were four major outages in RTGS systems during October 2014 to February 2021 (Table 1). Such outages are not indicative of a lack of resilience, but about getting systems back online in good time after disruptions. This involved: (i) the Reserve Bank Information and Transfer System (RITS) in Australia; (ii) the Trans-European Automated Real-time Gross Settlement Express Transfer System (TARGET2) in Europe; (iii) the Clearing House Automated Payment System (CHAPS) in the United Kingdom; and (iv) the Fedwire Funds Service in the United States. These payment systems handle large value transactions that are sizeable relative to national output and are linked to cross-border multi-currency systems such as CLS.

Table 1. Outage of Systemically Important Payment Systems in Selected Jurisdictions

Jurisdiction (Payment System)	Volume (millions)	Value of transactions (USD billions)	Average value per transaction (USD thousands)	Value of transactions as a percentage of GDP (%)	Outage (hours)
Australia (RITS)	13	36,629	2,889	2,642	<2
Euro Area (TARGET2)	89	509,382	5,733	3,813	10
United Kingdom (CHAPS Sterling)	49	106,358	2,186	3,766	9
United States (Fedwire)	168	695,835	4,149	3,200	3 to 4

Notes: Transaction figures are for 2019 based on data from the BIS. Outage hours are based on public information of operational incidents associated with the RITS in July 2020, TARGET2 in October 2020, CHAPS Sterling in October 2014, and Fedwire Funds Service in February 2021 (see Appendix 3). For RITS, annual assessments also reported operational incidents in February 2015 and August 2018.

Source: Bank for International Settlements; IMF staff.

International lessons could be drawn from the operational incidents in relation to improving the operational resilience of existing and emerging payment infrastructures and services.

A. Reliability Objectives

OROs such as recovery time objectives could be difficult to meet. OROs serve as benchmarks to evaluate performance and effectiveness against expectations. Critical information technology systems are expected to resume operations within two hours following disruptive events, as guided by international standards and oversight requirements. Nevertheless, operators were able to complete end-of-day settlements on the day of the disruption. Logistical challenges to ensure effective system failovers and movement of resources across primary and secondary sites were involved, for example.

Such experiences demonstrate the vulnerabilities of existing resiliency arrangements for electronic payment systems and the need for incident monitoring, timely reporting, cause-and-effect investigations, and public

disclosure of operational incidents.[15] Such circumstances could necessitate system operators and businesses to adjust strategies and operating and business models to be inherently flexible and resilient (IBM, 2020; IMF, 2020). Emerging practices suggest the setting of impact tolerances for each important business service and the identification and management of any risks to remain within the impact tolerance for each important business service (Bank of England, 2021).

A key question is whether existing resiliency arrangements would meet user expectations in the digital era. The greater demand for speed, rapid delivery times, and 24/7/365 payments availability in the digital era would imply higher expectations for uninterrupted service levels, which would appear difficult to achieve under existing resiliency arrangements.

B. Redundancies

Back-up systems fell short of commencing immediate operations following disruptive events. In highly complex cases involving multiple regions and sites, for example, backup systems located in the same region of the primary site failed to start and necessitated system administrators to move operations to a different region. The seamless transition from primary to back-up sites could also face delays from downtime periods that unavoidably interrupt operations.[16] The fact that such practices remain suggest that existing operational resiliency arrangements are insufficient to meet the objective of uninterrupted resiliency.

As the public becomes increasingly reliant on technology as part of their daily activities, authorities are also being expected to ensure public confidence. Consequently, this would require the appropriate anticipation and seamless response times from FMIs and payment service providers against any disruptions. The current redundancy arrangements that include primary and secondary sites-type of back-up systems appear to be inadequate to ensure resiliency in a real-time uninterrupted payment system. A further complication is staff unavailability, which could make redundancy arrangements in BCPs subject to resource constraints (CPMI, 2021; Cheney, 2006).

C. Critical Service Providers

Operational incidents were linked to critical service providers. For FMIs, operational reliability may be dependent on the continuous and adequate functioning of service providers that are critical to an FMI's operations, such as information technology and messaging providers.[17] While software failures were identified as the main cause of outages, problems were also associated with telecommunication services and other third-party service providers such as utilities.

[15] For example, the number and total duration of operational outages to retail payment services are reported by authorities in Australia (RBA, 2020). In Europe, the ECB President was involved in hearings and provided written responses to members of the European Parliament in relation to TARGET2.

[16] A benchmarking study found that 22 out of 24 central banks' information technology and systems departments were able to restore their operations after experiencing outages under 50 minutes on average or below their maximum acceptable downtime tolerance (Source: Centralbanking.com).

[17] Unless otherwise indicated by the relevant authorities, activities not directly related to essential operations of the FMI and utilities (such as basic telecommunication services, water, electricity, and gas) are out of scope when identifying critical service providers. Third parties could also generally include FMI participants, linked FMIs, service providers, vendors, and vendor products (Monetary Authority of Singapore, 2020; FSB, 2020b; CPMI-IOSCO, 2016).

Different economic sectors depend heavily on telecommunication services for their own business continuity and resiliency. Multiple telecommunication services could, however, also depend on the same energy source whereby energy failures could bring down the whole telecommunication service. Power outages could also affect multiple critical infrastructures and the cascading impacts that occur when one component falters.[18] The emerging use of cloud services could also increase the concentration risk if there is a narrow set of major providers used by the market (Reserve Bank of New Zealand, 2020).

As dependencies and vulnerabilities to critical service providers increase, the regulator, supervisor or overseer of an FMI and PSPs, may consider the assessment of such service providers against oversight expectations (CPMI-IOSCO, 2014). This should aim to provide assurance on the quality of services, and in the case of FMIs, compliance with the PFMI, where permitted under the applicable legal framework.

D. Endpoint Security

Cyber-attacks were ruled out from cause-and-effect investigations, particularly for operational incidents associated with SIPS. At the international level, authorities have been proactive in strengthening the cyber resilience of FMIs (CPMI-IOSCO, 2016). This has included efforts in improving governance arrangements, identification, protection, detection, response and recovery, testing, situational awareness, and learning and evolving.

An inter-related issue, however, is ensuring the endpoint security of wholesale payments. For example, such wholesale payments may be initiated or received by banks which are users of common messaging providers and participants in SIPS. Following international incidents, international efforts have been made to reduce the risk of wholesale payments fraud related to endpoint security. (CPMI, 2019). Similarly, efforts have also been made to promote strong customer authentication in retail payment services (particularly through the issuance of regulations in Europe).

E. Alternative Arrangements

One operational incident also illustrated the usefulness of having manual paper-based procedures as part of contingency plans. As guided by the PFMI, this forms part of alternative arrangements in BCPs to allow for the processing of time-critical transactions in extreme circumstances and helps complete settlement by the end of the day of the disruption. Such recommendations are largely applicable to SIPS and in circumstances where critical service providers and utilities continue to function normally under extreme circumstances (such as natural disasters).

However, in the event of wide scale and major disruptions that could cause prolonged outages to major public utilities and payment infrastructures (for several days or weeks due to a natural disaster), a common question is the role of cash in the national crises preparedness plan. As cash is not in the scope of this paper, we

[18] This was also evident in Hurricane Katrina case whereby one's processing systems may be functioning after a disaster, it is possible that its business partners' data systems may not (Cheney, 2006).

provide a summary of major issues and developments relating to contingency planning for future research (Appendix 4).

IV. Development and Operational Issues for the Future

This section explores development and operational issues, which should be guided by the PFMI and considered as part of business continuity management to improve operational resilience in existing and future payment systems. These issues relate to impact tolerance, business continuity arrangements, tandem processing, interoperability, and cost and implementation. As noted earlier, operational incidents illustrate how established objectives may not have been met. As guided by the PFMI, operational objectives should be periodically reviewed to incorporate new technological and business developments. Furthermore, appropriate adjustments should be made to BCPs and associated arrangements based on the results of testing exercises that address scenarios that simulate wide-scale disasters and inter-site switchovers.

A. Impact Tolerance

The first issue is setting impact tolerances in addition to establishing clear reliability objectives. For OROs, which are guided by the PFMI, this includes operational performance objectives and committed service-level targets. This could be both qualitative and quantitative. System availability (for example, 99 percent of operating hours) or RTO are examples of common quantitative targets used to ensure reliability objectives (while qualitative measures and examples are not publicly available). For systems currently with 2h-RTO, this is particularly important for SIPS and other FMIs, where practices have varied across jurisdictions (CPMI-IOSCO, 2021). They are also equally important to the critical service providers to such FMIs. Theoretically, operators may consider real-time recovery that could be made feasible with further technological advances (such as through tandem processing). It would be important that such resiliency requirements are set based on actual user needs and cost-benefit priorities.

Impact tolerances are distinct from RTO. This refers to the maximum tolerable level of disruption for an important business service, whereby further disruption could significantly threaten the transfer of payments or the safety and efficiency of the payment system. RTOs continue to apply where applicable and should be aligned earlier with business impact analysis and enterprise risk. Some jurisdictions (United Kingdom) have introduced such supervisory expectations for banks and supporting services, and expect operators (banks, third-party service providers) to flexibly set such impact tolerance levels for each business service and/or supporting service.[19]

Impact tolerance could be a time metric or include other factors such as the number of end-users impacted, or the volume or value of payments disrupted. This would require the identification of key business functions and supporting services (for example, from third-party service providers). For banks' business activities, this may relate to service offerings associated with settlement, custody, correspondent, and payment activities. Although impact tolerance provides specific metrics, recovery options and plans are still needed. If such key business

[19] See Bank of England (2021).

functions and supporting services have been identified as not being able to recover within the predefined impact tolerance, then steps are required to improve operational resilience.

In practice, when such key business and supporting services (from banks, third-party service providers) have interdependencies with SIPS or other FMIs, their impact tolerances would also need to consider the OROs and/or impact tolerance set for the latter entities. For example, a SIPS is expected under existing international standards to achieve a 2h-RTO following a disruptive event and ensure end of day settlement.[20] Otherwise, inter-day settlement exposures (especially for cross-border and multi-currency payment arrangements) could be a source of settlement risks and financial stability risks. Such an approach enables flexibility in setting separate impact tolerances for specific business services relative to distinct risk profiles and requires collective effort.

B. Business Continuity Arrangements

The second issue is identifying alternative arrangements to ensure recovery and business continuity. As noted, wide-scale or major disasters affecting payment systems and the necessary underlying infrastructures could arise from multiple scenarios. Recovery from such situations would be facilitated by factoring: (i) common, identical, and global standards for payments; (ii) common global payment systems with geographically dispersed processing sites; (iii) real-time copies of transaction and account databases in secure processing environments that have distinct risk profiles and are redundant; (iv) parallel satellite-based communication facilities (in addition to landline-based) for disaster situations; and (v) comprehensive local power-generation capabilities.

The physical security of payment system sites needs to be increased to reduce the risks from different kinds of attacks and natural catastrophes. For example, this could include employing to a larger extent physical underground sites, if practicable.

The comprehensive and effective implementation of common, global, and identical payment standards, as practiced for telecommunication services, would make it possible to use payment systems across different networks in the same way as mobile telephone systems. This would be the most important first step in improving resiliency. While common standards can provide interoperability, it does not guarantee a seamless switch over to other networks or arrangements. This depends on business and commercial agreements.

As payment systems would become global, this trend could accelerate. A global and common decentralized network-based payment system would be less vulnerable. Each processing node should be able to process transactions independently. This would require a coordinated structural design supporting decentralized payment processing.

Although most electronic payment systems require telecommunication services, only a limited are satellite-based. Providing satellite-based communications, at least for backup solutions, would reduce considerably the sole dependence on landline-based telecommunications, which are more prone to natural catastrophes than satellite-based solutions. This also helps mitigate potential single points of failure. As payment data volumes are limited, they could easily be transferred along more demanding satellite communication services.

[20] End of day settlement requirements could prove challenging in future global and round-the-clock operational environments, which would need to consider continuous settlement with finality.

Electronic payments will require electricity supply not only at service provider level, but also by the sender and receiver. The electricity capacity needed for payment instruments are rather limited and can be supplied with high-capacity battery, solar-electricity, small even man-powered generators etc. But without advanced preparations, it would be difficult to provide emergency electricity supplies during catastrophes.

For these kinds of disaster situations, it is important to establish payment system facilities outside the possible impacted areas which can, firstly, provide the necessary payment functionalities using the same standards and, secondly, have an updated complete set of payment account and transaction data, which can commence immediate payment processing.[21]

C. Tandem Processing

The third issue is considerations for tandem processing, which is a processing convention where each transaction is processed using two separate independent parallel processing streams. The two independent outcomes are checked against each other for correctness along the processing route. It could be viewed as an electronic version of the "four eyes" principle. This will provide rapid error detection and continuous back up and enable an automated failure correction solution aimed at facilitating seamless processing in the event of failure (Figure 5). Such parallel processing features make tandem processing distinct from redundant backups. Tandem solutions have often been implemented in different sub-components, but not within a whole payment system. From a social point of view, there has been a lack of sufficient incentives from industry to effect such changes. There are also cost and investment considerations (see below).

The main benefit of tandem processing is eliminating single point of failure structures in payment system software. Currently, hardware solutions are duplicated, triplicated or even several backup facilities are installed. However, there is only one payment processing, one payment account, one database management, and one payment telecommunication software for each service provider along the payment processing route from the sender to the receiver.

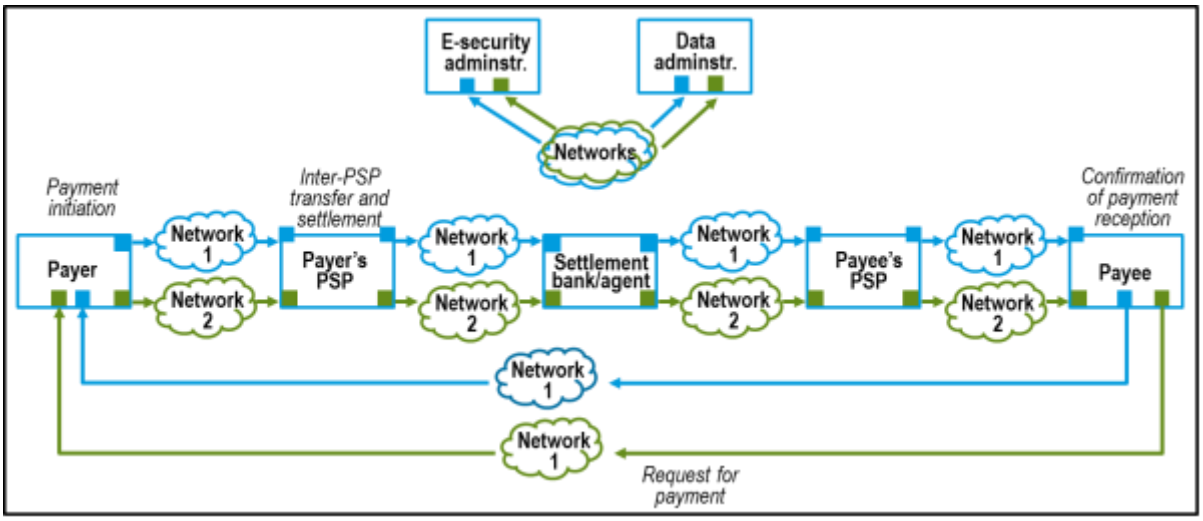
With a tandem-solution, payment processing could continue at each service provider given that at least the other of the two parallel systems would be operating. The risk for simultaneous malfunctions in two independent and highly resilient payment processing applications is very small. Building two independent systems controlling each other is a typical setup in industries where high availability and low failure risks requirements, such as in aviation and defense. The key features of tandem processing are further described below.

Duplicated independent network connections. In a resilient tandem-processing model, all network connections would be duplicated using completely independent networks as well as communication related software and hardware components. In normal times, all transactions would continuously be routed via both networks. If one networks fail, the connection will automatically fall back to solo-mode processing deploying available network. Transactions would be routed in parallel within each network to avoid failing nodes and connections. In this setup,

[21] The risks posed by natural disasters affect all sectors and have intensified with climate change (IMF, 2019). Among others, small island countries are highly vulnerable. Caribbean countries, for instance, have regularly experienced natural disasters. This included: Hurricane Maria in the Dominica Republic in 2017; Hurricane Dorian in the Bahamas in 2019; La Soufrière volcanic eruption in St. Vincent and the Grenadine's in 2021, which also affected Barbados. In such events, the financial sector has always been largely affected. For example, the Central Bank of Barbados closed its office and suspended in-person operations following the spread of severe volcanic ash. Investing in disaster-resilient infrastructure has therefore become critical for these countries.

payment routing is a built-in function within the payment network whereby each payment instruction is routed directly to beneficiary's PSP without central clearing involvement.

Figure 2. Synchronized Tandem Payment Processing Design



Source: IMF staff.

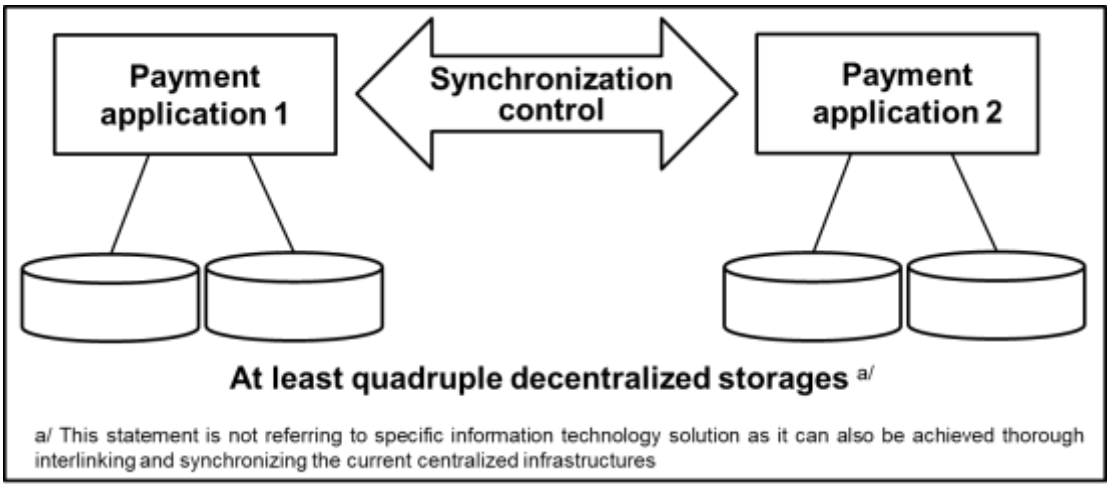
Duplicated independent software/hardware components. Each payment processing node consists of two parallel independent payment processing systems operated on independent hardware and software environment with different risk profile. Failure in one processing system in a node would automatically be responded by a fall back to solo processing by the uninterrupted node.

Automatic synchronization check. The parallel payment applications are equipped with automatic synchronization checks to compare outputs from both parallel processes (Figure 6). Automatic alert system should exist against failure to complete payment processing within reasonable time tolerance of any single component and thus alerting systems to fall back to solo-mode processing. Optimizing artificial intelligence-based algorithm would enable automatic analysis and error correction against possible output discrepancies between two applications prior to the switch.

Decentralized-based transactional data recording and storage with redundancy. Decentralized data recording and storage provides a secure way in producing mirrored copies of transaction information. Each application needs at least two separate transactional data recording. Real-time copies should also be kept at a secondary site with a different risk profile compared to the primary site. The secondary site can then take over transaction processing after transaction routing table has been automatically updated. The data administrator ensures data consistency across different copies stored in different databases (Figure 5).

Settlement as an integrated part of payment transaction processing. The settlement function sits in the middle of payers' and payee's PSPs (Figure 5). Settlement can be done by using commercial bank money or central bank money (including prospective CBDC). Real-time payments need immediate (and non-probabilistic) finality for all parties of transactions to reduce settlement and liquidity risk.

Figure 3. Synchronization Check Between Parallel Payment Applications



Resilient information security. Security applications in payment networks need to be seamlessly accessible without undermining efficiency. Transactions and information transfers in the payment network need to be strongly encrypted based on at least two different encryption systems. The security of the system should not be jeopardized by flaws or exposures of one of the encryption system(s). This helps address current shortcomings in identification and encryption systems, which are generally based on a single application or algorithm and lack alternatives if existing arrangements are not operating properly. While encryption provides confidentiality, security and risk management need to be integrated at all levels of the enterprise architecture. Activities like architecture risk analysis, threat modeling, specific types of application testing, integrations, and design also need to be practiced and enforced.

D. Interoperability

The fourth issue is facilitating global interoperability, which is important to facilitate tandem processing. Due to their history of establishment, traditional payment system infrastructures are characterized by a mix of non-interoperable and non-standardized proprietary local solutions. As a result, their service and resiliency levels vary considerably, are fragmented, and lack interoperability. Their cross-border usage facilities are inefficient when available. A rough estimate found at least 1,200 payment systems[22] operating worldwide. Most of which run under different software applications. Interoperability and tandem processing support payment processing, payment accounts, and database management that operate in parallel.

The above condition is observed for both private and public payment infrastructures. As an example, each RTGS system has different service levels and connectivity standards. Most of them are also built on non-interoperable software/hardware solutions which are incompatible for cross-border use, with the exceptions of a few off the shelf software-based RTGS systems.

[22] Assuming 150 independent payment areas, with average of eight separate payment systems on average in each area consist of each one credit transfer system, cheque clearing, online-payment system and RTGS, and each two card payment systems and mobile payment systems. However, in many countries there are even more payment system due to regional systems and bank group-based systems.

Resiliency needs interoperability at both domestic and cross-border levels and thus needs common standards.[23] This would improve cost efficiency, service levels, and availability. Building duplicated synchronized payment systems will require investments and maintenance costs. However, when payment systems are standardized and based on reusable programming libraries, this would reduce the costs of payment system development. As such achievements have been made in the telecommunications sector, it is technically possible for electronic payment systems to achieve similar goals as both are data transfer services.

If future payment systems and services would be globally standardized, central banks could, at best, provide backup services to each other and national payment volumes could in disaster scenarios be processed by unaffected payment infrastructures in neighboring or more far away countries. Payments are simple message and settlement transfers between sending and receiving accounts and customers. Globally interoperable systems would both reduce costs and increase resiliency.

Future cross-border payments, evolving technologies, and new business models would further accentuate the need to converge standards and oversight frameworks. Cooperative arrangements at the international level would need to be created to facilitate better information sharing and crisis management. If new systems are built and cross border payments increase, the potential contagion effect of a crisis could also magnify. Therefore, operational resilience must be built not just in the design of the systems but also simultaneously in the design of regulatory standards, messaging standards, and impact tolerances and crisis management protocols between the public and private sectors.

E. Cost and Implementation

The fifth issue is examining cost and implementation. Investments in resilience are sometimes seen as lacking cost-effectiveness during normal periods, but once a crisis arises, such previous expenditures demonstrate their benefits. Relevant studies have shown that investing in structural resilience could increase potential economic output, lower expected losses, and improve continuity of public services (IMF, 2019; Simison, 2019).

As noted earlier, efforts to effect strengthen operational resilience would require sufficient incentives. Building duplicated synchronized payment systems would require investments and maintenance costs. Investments costs are determined up front and are based on current offerings. Additionally, there would be maintenance and updating costs. Costs and benefits will also vary across countries depending on their financial structures and current systems. When payment systems are well standardized, the costs of development would fall. Currently, all payment service providers need to build (or buy) separate payment applications for each payment area (country) and for their own account system and hardware environment.

The traditional setup for cost-benefit analysis is to compare costs and benefits of given investments. For investments in operational resilience, this would vary based on the targeted level of resiliency as the consequences of actual failures will change. For example, the consequences in case of automatic immediate recovery would be smaller compared to recovery after two hours or next day. Electronic payment failures with shorter outages would directly affect electronic commerce with delayed orders processing restricting new orders.

[23] Common standards are sometimes seen as a barrier for development and innovation. In many cases for payment services, service providers have been reluctant to change their current systems and services. Providing new, common, and versatile standards could increase competition. This has happened in the telecom industry. It can also happen in the payment industry.

The larger the reliance of financial markets to immediate real-time payment-versus-payment and delivery-versus-payment settlement of currency and securities trading, the larger the impact of failure to financial markets. Liquidity supply would be disrupted and thus affect market rates.

As FMIs and PSPs could generally underinvest in their operational resilience as compared with what is perceived by their customers' and the public, authorities may need to consider regulations or sanctions to stimulate investment. Such remediation measures serve to ensure the safety and efficiency of payment systems, which are common public policy objectives. As it is important that a large share of all transactions, particularly time-critical transactions, can be processed in stress situations, this could translate to stricter resiliency requirements for FMIs and PSPs that process urgent payments. Differentiating resiliency requirements should focus investments decision on areas where benefits are larger.

V. Conclusion and Future Research

This paper examined lessons from major operational incidents in electronic payment systems and identified issues that could help strengthen their resilience. International experiences suggest that recovery time objectives could be difficult to meet. Strengthening operational resilience in payment systems means creating the capability to identify internal and external sources of risks and anticipating and preparing for wide-scale or major disruptions.

This paper argued that existing frameworks for operational resilience that rely on redundant back-ups are necessary, but insufficient, to ensure high oversight and user expectations in the digital era. As noted, new technologies, product and service offerings, and access points for payment initiation, are forming part of this digital transformation. Greater demand for speed, delivery, and availability would require uninterrupted and seamless services which is a shortcoming of existing redundancy models. While operational resiliency frameworks make use of OROs and impact tolerances, recovery and service availability targets, as well as interoperability requirements, future resiliency levels cannot be sufficiently achieved by relying on separate processing components and entities.

Development and operational issues were identified as part of further considerations to improve operational resilience and business continuity management in the future. These are five-fold, including: setting impact tolerances; identifying alternative arrangements to ensure recovery and business continuity; considering tandem processing to mitigate single points of failure structures in payment system software; facilitating global interoperability; and examining cost and implementation of resiliency investments.

Future research is needed. For instance, work may examine how central bank money, both in terms of physical cash and central bank digital currency infrastructures, would fit into the broader framework for operational resilience. Questions remain on how cash infrastructures should evolve under a digital crisis scenario, where there is a loss of public confidence in using electronic payments. Appendix 4 provides background on the role of cash in contingency planning. Also, how could new central bank digital currency infrastructures, if implemented, be designed to ensure operational resilience, or offer a possible alternative to traditional payment systems. The possibilities of tandem processing would also benefit from a deeper analysis from neutral external parties with expertise in information and communications technology.

References

Adelmann, F., Elliott, J.A., Ergen, I., Gaidosch, T., Jenkinson, N., Khiaonarong, J.T., Morozova, A., Schwarz, N., Wilson, C. (2020). "Cyber Risk and Financial Stability: It's a Small World After All", International Monetary Fund, Staff Discussion Note, December 7.

Aldasoro, I., Frost, J., Gambacorta, L., and Whyte, D. (2021). "Covid-19 and cyber risk in the financial sector", BIS Bulletin No.37, Bank for International Settlement, January 14.

Bank of England (2021). Supervisory Statement on Operational Resilience: Recognized Payment System Operators and Specified Service Providers, March.

_____ (2019). Sector Simulation Exercise: SIMEX 2018 Report, September.

_____(2015). Bank of England publishes independent review of RTGS outage. March.

Bank of England, Prudential Regulation Authority, the Financial Conduct Authority (2021). Operational resilience: Impact tolerances for important business services, March.

Bank of Japan (2011). Responses to the Great East Japan Earthquake by Payment and Settlement Systems and Financial Institutions in Japan. Bank of Japan Report and Research Papers, Payment and Settlement Systems Department, Bank of Japan, Tokyo.

Basel Committee on Banking Supervision (2021). Principles for Operational Resilience, March.

Bech, ML., and Garratt, R.J. (2012). Illiquidity in the Interbank Payment System Following Wide-Scale Disruptions, Journal of Money, Credit and Banking, Vol. 44, No. 5, August, 903-929.

Board of Governors of the Federal Reserve System., Office of the Comptroller of the Currency., Securities and Exchange Commission. (2002). Interagency Paper on Sound Practices to Strengthen the Resilience of the U. S. Financial System. April 7.

Cantelmo, A., Melina, G., Papageorgiou, C. (2019). "Macroeconomic Outcomes in Disaster-Prone Countries", IMF Working Paper (WP/19/2017), International Monetary Fund, Washington, D.C, October.

Carbon Black (2021). "The State of Incident Response 2021".

Carnegie Endowment for International Peace (2021). "Timeline of Cyber Incidents Involving Financial Institutions".

Cheney, J.S. (2006). "The Role of Electronic Payments in Disaster Recovery: Providing More Than Convenience", in The Role of Electronic Payments in Disaster Recovery: Providing More Than Convenience conference summary, Federal Reserve Bank of Philadelphia, May 3-4.

Cleland, V. (2021). A New Dawn for Payments. Speech at the City Week, 21 June.

Committee on Payments and Market Infrastructures and International Organization of Securities Commissions (2021). Implementation Monitoring of PFMI: Level 3 Assessment of Financial Market Infrastructures' Business Continuity Planning, July.

_____ (2019). Reducing the Risk of Wholesale Payments Fraud Related to Endpoint Security: A Toolkit, October.

Committee on Payments and Market Infrastructures and International Organization of Securities Commissions (2016). Guidance on Cyber Resilience for Financial Market Infrastructures, June.

_____ (2014). “Principles for Financial Market Infrastructures: Assessment Methodology for the Oversight Expectations Applicable to Critical Service Providers”, Bank for International Settlements, December.

Committee on Payment and Settlement Systems and International Organization of Securities Commissions (2012a). “Principles for Financial Market Infrastructures”, Bank for International Settlements, April.

_____ (2012b). Principles for Financial Market Infrastructures—Disclosure Framework and Assessment Methodology, Bank for International Settlements, December.

Committee on Payments and Market Infrastructures and World Bank (2020). “Payment Aspects of Financial Inclusion in the Fintech Era”, April 14.

Deloitte (2015). Independent Review of RTGS Outage on 20 October 2014, March 25.

De Nederlandsche Bank (2020). “The role and future of cash”, De Nederlandsche Bank, Eurosystem, December.

Essuman, D., Nathaniel, B., and Jonathan, A. (2020). “Operational Resilience, Disruption, and Efficiency: Conceptual and Empirical Analyses”, International Journal of Production Economy, November.

European Central Bank (2021a). Best Practices Applied by Financial Market Infrastructures in their Business Continuity Plans During the COVID-19 Pandemic.

_____ (2021b). TARGET Annual Report 2020.

_____ (2021c). TARGET2-Securities Annual Report 2020.

_____ (2021d). Letter from the ECB President to Mr Markus Ferber, MEP, on TARGET2, January 27.

_____ (2020a). Letter from the ECB President to Mr Martin Schirdewan Member of the European Parliament, on TARGET2, December, 20.

_____ (2020b). Press release: “ECB announces independent review of payments system outage”. November 2020

_____ (2020c). TARGET Annual Report 2019

_____ (2020d). Eurosystem Oversight Framework for Electronic Payment Instruments, Schemes and Arrangements: Draft for Public Consultation. October.

European Commission (2020). Regulation of the European Parliament and of the Council on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014, 24.9.2020.

_____ (2017). Joint Report to the European Parliament and the Council on the Implementation of the Joint Framework on Countering Hybrid Threats—A European Union Response, July 19.

European Parliament (2017). “On Fintech: The Influence of Technology on the Future of the Financial Sector”, Committee on Economic and Monetary Affairs, A8-0176/2017, April 28.

European Systemic Risk Board (2020), “Systemic Cyber Risk”, European System of Financial Supervision, February.

Financial Service Authority, HM Treasury, Bank of England (2008). “UK Financial Sector Market Wide Pandemic Exercise 2006 Progress Report”, May.

Financial Stability Board (2020a). “The Implications of Climate Change for Financial Stability”, November 23.

_____ (2020b). Regulatory and Supervisory Issues Relating to Outsourcing and Third-Party Relationships: Discussion paper, November 9.

_____ (2013). “Recovery and Resolution Planning for Systemically Important Financial Institutions: Guidance on Identification of Critical Functions and Critical Shared Services”.

Monetary Authority of Singapore (2020). Financial Institutions Need to Review Security Controls Amidst COVID-19: MAS’ Cyber Security Advisory Panel, November 10.

Fjader, C., Helwig, N., and Wigell, M. (2021). “Recognizing Geoeconomic Risk: Rethinking Corporate Risk Management for the Era of Great-Power Competition”, Finnish Institute of International Affairs, Briefing Paper, June.

Fleming, M.J., and Garbade, K.D. (2002). "When the Back Office Moved to the Front Burner: Settlement Fails in the Treasury Market after 9/11," Economic Policy Review, Federal Reserve Bank of New York, vol. 8, November, pages 35-57.

Greenspan, A. (2008). The Age of Turbulence—Adventures in a New World, Penguin Books.

IBM (2021). “Operational Resilience Challenges in Banking and Financial Markets”. IBM Institute for Business Value, March 10.

_____ (2020). Resilience in the New Age of Risk: Anticipating the Unexpected. Expert Insights, IBM Institute for Business Value, August.

International Monetary Fund (2020). Norway: Financial Sector Assessment Program—Technical Note on Cybersecurity Risk Supervision and Oversight, August 12.

_____ (2019a). Building Resilience in Developing Countries Vulnerable to Large Natural Disasters, IMF Policy Paper, April 4.

_____ (2019b). Singapore: Financial Sector Assessment Program-Detailed Assessment of Observance of the CPSS-IOSCO Principles for Financial Market Infrastructures, June 24.

_____ (2016a). Small States’ Resilience to Natural Disasters and Climate Change—Role of the IMF, IMF Policy Paper, November 4.

_____ (2016b). Kingdom of Bahrain: Financial Sector Assessment Program—Detailed Assessment of Observance Assessment of Observance of the CPMI-IOSCO Principles for Financial Market Infrastructures, June 16.

_____ (2015a). Bosnia and Herzegovina: Financial Sector Assessment Program-Detailed Assessment of Observance of the CPMI-IOSCO Principles for Financial Market Infrastructures, August 3.

_____ (2015b). Norway: Financial Sector Assessment Program—Technical Note on Oversight and Supervision of Financial Market Infrastructure, and Selected Issues in the Payment System, September 17.

_____ (2006). “The Global Economic and Financial Impact of an Avian Flu Pandemic and The Role of The IMF”, February 28.

Lacker, Jeffrey M. (2004). “Payment System Disruptions and the Federal Reserve Following September 11, 2001”. Journal of Monetary Economics, 51, 935-65.

Mastercard Clearing Management System (2021). PFMI Disclosure Report by Mastercard Europe SA May 6

_____ (2020). Mastercard Incorporated Fiscal Year 2019 Form 10-K Annual Report.

Norges Bank (2021). Financial Infrastructure Report.

Owens, C., Craig, L., and Yates, J. (2019). “The Blackout Report”, Riello UPS, Ltd.

Price Waterhouse Coopers (2020). “Travelex completes debt restructuring”, August 6.

Ranghieri, F. and Ishiwatari, M. (2014). “Learning from Mega Disasters—Lessons from the Great East Japan Earthquake”, World Bank.

Reserve Bank of Australia (2021). Assessment of the Reserve Bank Information and Transfer System, May.

_____ (2020). Payment System Board Annual Report.

Reserve Bank of New Zealand (2020). “Consultation Document: Risk Management Guidance on Cyber Resilience and Views on Information Gathering and Sharing”, October 20.

Simison, B (2019). “Investing in Resilience”, Finance & Development, Volume. 56, No. 4, International Monetary Fund, Washington, D.C, December.

Solheim, J.A. and Strømme, H. (2004). Upgrading and Outsourcing Norges Bank’s Settlement System, Norges Bank Economic Bulletin, Q2, 58-63.

Tiernan, A., Drennan, L., Nalau, J., Onyango, Morrissey, E.L., Mackey, B. (2019). “A Review of Themes in Disaster Resilience Literature and International Practice Since 2012”, Policy Design and Practice, 2:1, 53-74.

U.S. Department of the Treasury, Financial and Banking Information Infrastructure Committee, Financial Services Sector Coordinating Council, and Securities Industry and Financial Markets Association (2008). The FBIIC/FSSCC Pandemic Flu Exercise of 2007 After Action Report—U.S. Financial Services Sector Exercise Results, January.

Visa Europe Ltd. (2019). VEL CEO Letter to The Rt Hon. Nicky Morgan MP, Chair of the Treasury Committee, 15 June 2018; PFMI Public Disclosure of Visa Europe Limited’s Self-Assessment: Self-Assessment Submitted to The Bank of England (as Authority Overseeing Visa Europe), August 3.

Wakatabe, M. (2019). Financial and Settlement Systems as Social Infrastructure: Disaster Management Perspective. Opening Remarks at the Symposium “The Impact of Natural Disasters on Financial Markets and Financial Institutions”. Held at Nagoya University Graduate School, November 28, Bank of Japan.

Watne, K. (2012). “A New Settlement System at Norges Bank. Norges Bank Economic Bulletin”, Vol. 83, 4-13.

Appendix 1. Key Challenges for Improving Operational Resilience in Payment Systems

Efforts to improve operational resiliency are confronted with the following challenges: (i) technical complexity; (ii) organizational complexity; (iii) dependence on single software versions; (iv) dependence on external infrastructures; (v) vulnerability of information security solutions; (vi) geographical, jurisdictional, and time-zone issues; and (vii) insufficient incentives for resiliency.

Technical complexity. In online and real-time infrastructures, transactions are processed individually involving several applications from several service providers. Each of application and service provider utilize different components[24]. Most of these are acquired from external sources based on outsourcing agreements, to a large extent. Many of these components are duplicated in different parts of the payment processing chain e.g., a database manager software can be employed by several partners. A failure in one underlying technical component can thereby affect several parties. Problem exist when failure in a party or a critical component might completely halt the processing chain. As many components involved the overall chain, the probability of failure is growing. The effects on customers are immediately apparent in online and real-time systems.

Organizational complexity. More parties are involved in the processing chain and most of them rely on outsourcing e.g., software developments, telecommunication services, security solutions, payment instrument production (chip-cards, e-banking user facilities etc.). There seems to be a lack of overall resiliency responsibility as it depends on the resiliency level of each individual component. Complexity is even larger with globalization and would not be sufficient to handle continues processing, there is a need for specialized organizational solutions to enable an immediate action against major disruption through local and international coordination. Deciding on parties who is held responsible to find actual problem and fix it would be much harder as technical and organizational complexity are rising.

Dependence on single software versions. The current payment software is mostly running in one operating system environment. Most PSPs' system design is characterized with single payment software developed by single developer with single database management system. Any undetected errors/bugs in software or supporting database will require a roll back to the previous version of the software (or fixing or circumventing the bug in the current version) to acquire redundancy copy. This process would be time consuming and complex, especially when major software changes are made within the last update. The risks for internal bugs increase with growing system complexity.

Dependence on external electronic infrastructures. E-payments rely heavily on electricity and telecommunication networks. Although, the overall quality of these services has improved over the years, idiosyncratic risk like climate change due partly to global warming can impose uncertainty in the availability and failure rates of these infrastructures. Readiness for the backup solutions for these infrastructures would be important to complete the processing chain.

Vulnerability of information security solutions. Ransomware incidents have been increasing. Cybercriminals have increased their efforts and investments for bypassing different kinds of security and privacy solutions. Severe security breaches will require closing affected systems and services partly and for shorter or longer periods. Typical examples in the past have been replacing off-line ATM systems with online systems because cybercriminals have learnt how to forge off-line cards. Well-organized terrorist/criminal attacks on electronic payment systems can potentially result in major unrecoverable losses due to fraudulent transactions. The

[24] This consist of server equipment (and sometimes mainframes), which contain different operating systems and middleware applications, database manager software (and sometimes separate servers), telecommunication software (and sometimes separate servers), different information security firewalls/servers and the actual payment processing software.

openness and anonymity set up within current internet services provide criminals and terrorists opportunities to attack with limited risks of being detected. Extensive investments and restructuring in information security solutions would be needed to protect payment systems.

Geographical, jurisdictional, and time-zone issues. Geographical proximity of backup sites will increase risks. Domestic PSPs will have less control on payment service resources and employment with the increasing use of cross-border payments and offshore outsourcing partners, cloud computing etc. Smaller PSPs in developing countries will probably have less bargaining power compared to larger competitors in the event of failure. In addition, conflicting rules and regulations (e.g., finality, prefunding etc.) may occur if payment transactions are processed in different jurisdictions. The fourth era of payment systems will operate continuously 24/7, in multicurrency mode and thereby without time-zones and end-of-day timings. This will require new type of solutions and open hours for settlement systems like central banks RTGS systems.

Insufficient incentives for resiliency improvements. Private service providers are generally less risk-averse compare with their customers and society in general. Aside from their profit motive, they tend to maximize transaction volumes and underinvest, for instance, in costly backup, security and similar solutions until the decision becomes necessary due to competition or regulatory requirements. Consequently, different kinds of failures may occur.

Appendix 2. Principles Relevant for Assessing Operational Resilience in Payments

CPSS-IOSCO Principles for Financial Market Infrastructures—Operational Risk

Principle 17: Operational Risk *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 fulfilment of the FMI's obligations, including in the event of a wide-scale or major disruption.*	
Key Considerations	
1	An FMI should establish a robust operational risk-management framework with appropriate systems, policies, procedures, and controls to identify, monitor, and manage operational risks.
2	An FMI's board of directors should clearly define the roles and responsibilities for addressing operational risk and should endorse the FMI's operational risk-management framework. Systems, operational policies, procedures, and controls should be reviewed, audited, and tested periodically and after significant changes.
3	An FMI should have clearly defined operational reliability objectives and should have policies in place that are designed to achieve those objectives.
4	An FMI should ensure that it has scalable capacity adequate to handle increasing stress volumes and to achieve its service-level objectives.
5	An FMI should have comprehensive physical and information security policies that address all potential vulnerabilities and threats.
6	An FMI should have a business continuity plan that addresses events posing a significant risk of disrupting operations, including events that could cause a wide-scale or major disruption. The plan should incorporate the use of a secondary site and should be designed to ensure that critical information technology (IT) systems can resume operations within two hours following disruptive events. The plan should be designed to enable the FMI to complete settlement by the end of the day of the disruption, even in case of extreme circumstances. The FMI should regularly test these arrangements.
7	An FMI should identify, monitor, and manage the risks that key participants, other FMIs, and service and utility providers might pose to its operations. In addition, an FMI should identify, monitor, and manage the risks its operations might pose to other FMIs.

Source: CPSS-IOSCO (2012a).

CPSS-IOSCO Principles for Financial Market Infrastructures—Questions for Assessing Operational Resilience of Payment Systems

Key Considerations and Questions	
3	An FMI should have clearly defined operational reliability objectives and should have policies in place that are designed to achieve those objectives. *1. What are the FMI's operational reliability objectives, both qualitative and quantitative? Where and how are they documented?* *2. How do these objectives ensure a high degree of operational reliability?* *3. What are the policies in place that are designed to achieve the FMI's operational reliability objectives to ensure that the FMI takes appropriate action as needed?*

6	An FMI should have a business continuity plan that addresses events posing a significant risk of disrupting operations, including events that could cause a wide-scale or major disruption. The plan should incorporate the use of a secondary site and should be designed to ensure that critical information technology (IT) systems can resume operations within two hours following disruptive events. The plan should be designed to enable the FMI to complete settlement by the end of the day of the disruption, even in case of extreme circumstances. The FMI should regularly test these arrangements. Objectives of business continuity plan *1. How and to what extent does the FMI's business continuity plan reflect objectives, policies and procedures that allow for the rapid recovery and timely resumption of critical operations following a wide-scale or major disruption?* Design of business continuity plan *2. How and to what extent is the FMI's business continuity plan designed to enable critical IT systems to resume operations within two hours following disruptive events, and to enable the FMI to facilitate or complete settlement by the end of the day even in extreme circumstances?* *3. How is the contingency plan designed to ensure that the status of all transactions can be identified in a timely manner, at the time of the disruption; and if there is a possibility of data loss, what are the procedures to deal with such loss (for example, reconciliation with participants or third parties)?* *4. How do the FMI's crisis management procedures address the need for effective communications internally and with key external stakeholders and authorities?* Secondary site *5. How does the FMI's business continuity plan incorporate the use of a secondary site (including ensuring that the secondary site has sufficient resources, capabilities, functionalities and appropriate staffing arrangements)? To what extent is the secondary site located a sufficient geographic distance from the primary site such that it has a distinct risk profile?* *6. Has the FMI considered alternative arrangements (such as manual, paper-based procedures or other alternatives) to allow the processing of time-critical transactions in extreme circumstances?* Review and testing *7. How are the FMI's business continuity and contingency arrangements reviewed and tested, including with respect to scenarios related to wide-scale and major disruptions? How frequently are these arrangements reviewed and tested?* *8. How does the review and testing of the FMI's business continuity and contingency arrangements involve the FMI's participants, critical service providers and linked FMIs as relevant? How frequently are the FMI's participants, critical service providers and linked FMIs involved in the review and testing?*
7	An FMI should identify, monitor, and manage the risks that key participants, other FMIs, and service and utility providers might pose to its operations. In addition, an FMI should identify, monitor, and manage the risks its operations might pose to other FMIs. Risks to the FMI's own operations *1. What risks has the FMI identified to its operations arising from its key participants, other FMIs, and service and utility providers? How and to what extent does the FMI monitor and manage these risks?* *2. If the FMI has outsourced services critical to its operations, how and to what extent does the FMI ensure that the operations of a critical service provider meet the same reliability and contingency requirements they would need to meet if they were provided internally?*

	Risks posed to other FMIs *3. How and to what extent does the FMI identify, monitor and mitigate the risks it may pose to another FMI?* *4. To what extent does the FMI coordinate its business continuity arrangements with those of other interdependent FMIs?*

Source: CPSS-IOSCO (2012b).

BCBS Principles for Operational Resilience

Principle	Considerations
Governance	Utilizing existing governance structure to establish, oversee and implement an effective operational resilience approach that enables response and adaptation to, as well as recovery and learning from, disruptive events to minimize their impact on delivering critical operations through disruption.
Operational risk management	Leveraging on respective functions for the management of operational risk to identify external and internal threats, promptly assessing the vulnerabilities of critical operations and managing the resulting risks.
Business continuity planning and testing	Establishing business continuity plans and conducting business continuity exercises under a range of severe but plausible scenarios to test the ability to deliver critical operations through disruption.
Mapping interconnections and interdependencies	Mapping internal and external interconnections and interdependencies that are necessary for the delivery of critical operations once such operations have been identified.
Third-party dependency management	Managing dependencies on relationships, including those of, but not limited to, third parties or related entities, for the delivery of critical operations.
Incident management	Developing and implementing response and recovery plans to manage incidents that could disrupt the delivery of critical operations in line with risk appetite and tolerance for disruption. Incident response and recovery plans should be continuously improved by incorporating lessons learned from past incidents.
ICT including cyber security	Ensuring resilient ICT including cyber security that is subject to protection, detection, response and recovery programs that are regularly tested, incorporate appropriate situational awareness and convey relevant timely information for risk management and decision-making processes to fully support and facilitate the delivery of critical operations.

Source: BCBS (2021).

Appendix 3. Selected Operational Incidents in Payment and Settlement Services

Systemically Important Payment Systems[25]
Australia
Incident: On July 6, 2020, the Reserve Bank of Australia's RITS was affected by a power outage to the data center at the Bank's Business Resumption (BRS) site. The incident took place at 7.30 am. The majority of RITS services were re-established and fully operational from the RBA's primary site around 9 am and within the two-hour RTO. The opening of the RITS Daily Settlement Session was delayed from 9.15 am to 9.30 am. All transactions were able to settle as expected from that time. There was no downtime to the RBA's fast settlement service. **Cause:** Operational error. The power supply to the BRS data center hosting RITS infrastructure was inadvertently shut off during fire control system maintenance. An internal review identified a legacy switchboard design issue and a maintenance contractor failing to comply with procedures. **Impact:** RITS availability was affected but no widespread spillover was reported. RITS processes high-value interbank payments, including fast settlement service and currently has 167 participants, of which 102 are exchange settlement account holders, including the RBA. **Response:** RBA upgraded the switchboard involved in the incident, implemented enhanced contractor induction arrangements, and improved oversight of compliance with procedures by contractors. RBA is also establishing new service delivery arrangements for its facilities aimed to improve the approach to planning, risk assessment, and oversight of maintenance activities over the long term. This includes an increased role for staff with relevant engineering expertise to review changes as part of an enhanced internal engineering and advisory function. The RBA's annual assessment of RITS also recommended completion of this work in order to improve RITS observance against PFMI Principle 17 on operational risk. **Other:** In a separate incident during the assessment period, software supporting certain backup processes was mistakenly removed in the process of a broader system update. The incident did not have any direct operational impacts on RITS, and the software was reinstated once the error was detected. In another incident on June 17, 2021, RBA cancelled a bond purchase operation after outages. The issue appears to have originated in the systems of Akamai, a provider of internet services including content delivery and cloud computing.
Europe
Incident: On October 24, 2020, the European Central Bank's TARGET2 system was down for around 10 hours. All settlement services became unavailable with the backup system failing to boot up as failover to a secondary disaster recovery site took many hours. Consequently, no payment, ancillary system instructions or liquidity transfers from/to TIPS and T2S could be processed for several hours. **Cause:** Software defect at a third-party network device. Cyber-attacks were excluded. **Impact:** The glitch resulted in a drop in deposits worth more than EUR 400 billion (USD 473 billion). **Response:** ECB announced an independent review. The review would investigate the cascade of failures and seek to publish key lessons by the second quarter of 2021. The investigation would include the business continuity model, recovery testing, change management, and communication.

[25] Due to the lack of a single source of information at the international level that monitors, records, and discloses operational incidents on payment and settlement services, this compilation is based on publicly available information from official, company, and media sources.

Other: TARGET2 experienced earlier and separate incidents, although the failover to the secondary site was successful. In 2019, there were technical issues that led to a delay in the delivery of outgoing messages from TARGET2. On 11 August 2020, TARGET2 was down again and affected T2S due to human error.
Incident: On July 12, 2018, Mastercard experienced an outage that lasted more than one and a half hours. The incident caused some card payments to fail and affected many international banks. **Cause:** No public information is available. **Impact:** No public information is available. **Response:** No public information is available. Mastercard issued an email statement at the day of the incident to confirm the situation has been fully resolved and all transactions resumed as normal.
Incident: On June 1, 2018, Visa Europe Ltd (VEL) experienced a hardware failure that led to a partial outage lasting around 8 hours and affected 5.2 million card transactions across Europe. **Cause:** Hardware failure. The problem was with authorization, which was supposed to be sent to a chip and pin machine when transactions occur. **Impact:** Around 5.2 million card transactions across Europe were affected. Many Visa cardholders were inconvenienced with travel, grocery payments, and cash withdrawals. Banks and commerce groups advised customers to use cash or other payment cards. Consequently, some ATMs in the United Kingdom were already out of cash within a couple of hours. **Response:** VEL ordered an internal and independent third-party review to identify areas for improvement and to recommend remedial actions relating to its operational resilience, recovery, and response procedures. VEL established a work program to oversee the actions corresponding to the recommendations per the independent third-party review alongside internal findings.
United Kingdom
Incident: On October 20, 2014, the Bank of England's CHAPS experienced an outage of over 9 hours. This was caused by the introduction of defects as part of functionality changes made to the CHAPS in April 2013 and May 2014. **Cause:** Configuration changes triggered a previously undetected design defect. **Impact:** The outage effectively froze GBP 277 billion (USD 447 billion) worth of payments, which included all transactions submitted through CHAPS and put 700 time-critical housing market transactions on hold. **Response:** A commission ordered an independent review into the causes of the incident. The findings were presented to the Bank of England's Court. A full report with response was published in March 23, 2015.
United States
Incident: On February 24, 2021, the Federal Reserve's Fedwire Funds Service experienced a disruption around 3 to 4 hours. The outage also affected 14 other services, including Check 21, FedCash, Account Services, Central Bank and several FedLine services. **Cause:** Operational error. Cyber-attacks were excluded. **Impact:** No public information is available. Based on media sources, the outage also caused several cryptocurrency exchanges, including Gemini, Kraken and Coinbase, to experience delays.

Response: According to a statement from the Federal Reserve, it took steps to help ensure the resilience of the Fedwire and NSS applications, including recovery to the point of failure. No further details were provided. Fedwire resumed normal operations after the 3 to 4 hours outage.

Other: In separate incidents, the Federal Reserve experienced two significant service disruptions in 2019 and December 2020. Another incident involved an internal technical issue that took down the Fedwire Funds Service for about 3 hours in April 2020.

Payment, Currency, and Messaging Services

International

Incident: On December 31, 2019, Travelex online currency services was forced to shut down and was vulnerable for 8 months. Travelex trades in over 80 currencies and operates in more than 50 countries and across multiple stores (and ATMs) around the world. The company also provides outsourcing services for partners including banks, supermarkets, and travel agencies.

Cause: Cyber-attack (ransomware, e.g. REvil or Sodinokibi through unpatched Pulse Secure VPN servers).

Impact: The attack affected customers in 21 countries and the company's clients, including HSBC, RBS, Lloyds, Barclays, First Direct, Virgin, Clydesdale, and Tesco Bank. The attackers claimed they accessed a large volume of customer data (including dates of birth, national insurance numbers, credit card information) and demanded a ransom of USD 6 million.

Response: No known significant remedial action taken to improve resiliency after the attack. Travelex paid the hackers the equivalent of USD 2.3 million and completed a restructuring deal in August 2020. This delivered GBP 84 million (USD 119 million) of new money and substantially deleveraged the new group.

Incident: On February 4, 2016, a group of unidentified hackers attempted to steal USD 951 million from the Bangladesh Bank.

Cause: Wholesale payments fraud related to end-point security. The intruders used malware to obtain legitimate SWIFT credentials and signed into the network. SWIFT's core network was not compromised.

Impact: Five out of 35 fraudulent instructions were issued by security hackers through the SWIFT network. This led to the transfer of USD 101 million from Bangladesh Bank's account held at the Federal Reserve Bank of New York. USD 20 million was traced to Sri Lanka. USD 81 million ended up in the Philippines.

Response: SWIFT introduced mandatory security measures, including daily reports of customers' SWIFT activity and the Customer Security Program. The program was expanded in May 2017 with the launch of the SWIFT Information Sharing and Analysis Centre, which includes details of malware and intelligence gleaned from SWIFT's investigations into attempted cyber-attacks on its customers.

Zimbabwe

Incident: On July 2019 and July 2020, Zimbabwe's Econet Wireless experienced a power outage of 8 hours.

Cause: Utility failure. Generators at the company's operations center failed to kick in after a constant disruption of electricity power supply. Lake Kariba was affected by a drought, which reduced hydroelectric production and forced load shedding for 18 hours.

Impact: The incident hit 6.7 million active users in the country. A power cut to Econet's servers meant that 70 percent of Zimbabweans had no phones, internet, and mobile money services. This consequently had detrimental effects on the country's economy, as most financial systems halted because the country's economy runs through electronic systems and mobile money.

Response: Econet made an investment decision on Tesla batteries to reduce its reliance on generators. The company currently has 520 lithium-ion batteries that are used to provide back-up power at its 1,300 base stations. The investment had cut reliance on diesel-run generators by 75 percent.

Source: Bank of England (2015); European Central Bank (2021b; 2021c; 2021d; 2020a; 2020b; 2020c); Federal Reserve; Reserve Bank of Australia (2021); Deloitte (2015); Mastercard Clearing Management System (2021; 2020); Price Waterhouse Coopers (2020); Visa Europe Ltd. (2019); Bloomberg; Centralbanking.com; CNBC; Financial Times; Guardian; Paypers; Quartz Africa; Reuters; Risk Net; Sun; Wall Street Journal.

Appendix 4. Role of Cash in Contingency Planning

Cash has played an important role in national crises preparedness plans in some countries. Being public money, cash acts as legal tender, as a means of payment guaranteeing privacy, and is the only form of money that can be carried or kept as savings independently of a bank and as a fallback and alternative option if electronic payment systems failed. Cash is so far the only type of money that has the ability to provide immediate security for payments, allow for payments without the involvement of third parties, is independent from central verification, and is less dependent on electronic systems (as ATM and over the counter cash withdrawals at PSPs may still require electricity to function effectively). For wide-scale or major disasters, there may be a sudden peak in the demand for cash due to rising uncertainty (see Appendix 3). Reliance on cash may even be higher if public confidence in electronic payments is lost due to the recurrence of outages, system failures, cyber-attacks, and natural disasters.

Cash infrastructures could also be considered critical infrastructures. The absence of non-digital fallback plans, such as cash, could expose economies with significant risks from a system failure or cyber-attack. For example, the European Systemic Risk Board warns against the risks of disruptions in digital systems and argues that this could potentially threaten financial stability and possibly even cause a systemic crisis. In Sweden, the central bank has concluded that cash needs to be both protected and supplemented with a digital alternative and that there should be enough cash in case electronic systems break down (no decision has yet been taken to issue e-krona). For emerging and developing economies with rudimentary payment and telecommunications infrastructures and vulnerable to natural disasters, identifying cash as critical infrastructures is also relevant. [26]

Cash infrastructures also need to have operational resilience. Central banks and relevant stakeholders need to find the right balance between cost savings and maintaining continuity. The decentralization of money processing (counting, sorting, checking, and recirculating) by banks and/or licensed operators could improve efficiency. It would also make money processing infrastructures more robust in the event of disruptions. Maintaining the continuity of security transports to ATMs is also a concern from a security perspective as an essential element to ensure the accessibility and availability of cash. Central banks also need to have knowledge of market operator BCPs throughout the chain in view of its task to ensure the smooth operations.

For cash to function as an effective back-up and accommodate sudden surges in demand requires sufficient ATMs and capacity to replenish them more frequently. Against this backdrop, some countries have set a minimum number of ATMs that operate within their territory. The Dutch central bank sets 4,000 ATMs as the minimum number to ensure adequate access to cash services. The Swedish government passed a law requiring the largest banks to continue to provide adequate access to cash and requiring the Swedish central bank to have sufficient locations for professional parties to obtain banknotes. A separate channel for withdrawing cash could also be made over the counters at other PSPs.

A crisis management framework could also guide the deployment of cash as a fall back plan. Central banks could provide certainty to market participants in a timely manner and be continuously well-informed about the effectiveness of cash supplies and distribution. For example, the Federal Reserve addressed panic following September 11 by reassuring banks and armored carriers about the ample availability of currency for withdrawal, extending hours of operation, and arranging special deliveries. Fees that applied to certain banks accessing Fed cash services were also waived.

Source: De Nederlandsche Bank (2020); European Systemic Risk Board (2020); Lacker (2003).

[26] For example, such economies may have blank spots in remote areas, where there is a lack of fixed broadband networks (fiber-optic or landline telephone networks) and mobile data signals.