



TECHNICAL

NOTES & MANUALS

Business Continuity Planning for Government Cash and Debt Management

Emre Balibek, Ian Storkey, and H. Hakan Yavuz

TECHNICAL NOTES AND MANUALS

Business Continuity Planning for Government Cash and Debt Management

Prepared by Emre Balibek, Ian Storkey, and H. Hakan Yavuz

Business continuity planning is a critical part of government cash and debt management to ensure efficient and timely delivery of government services. Yet, many countries struggle to put in place an adequate business continuity plan (BCP) that covers government cash and debt management functions. This technical note and manual (TNM) aims to provide guidance on the steps that countries can follow to address this shortcoming. In doing so, it addresses the following issues:

- How can government cash and debt management units develop and implement a practical business continuity plan (BCP)?
- How can the process of developing a BCP be simplified economizing the use of resources?
- How has the nature of the business disruption risks and the landscape faced by cash and debt management evolved over the last decade? What solutions have emerged to maintain business continuity?
- How has the recent COVID-19 pandemic affected business continuity planning?

By focusing on the above questions, the TNM updates approach presented in the IMF TNM 1105 on “Operational Risk Management and Business Continuity Planning for Modern State Treasuries.”

Fiscal Affairs Department

Business Continuity Planning for Government Cash and Debt Management

Prepared by Emre Balibek, Ian Storkey, and H. Hakan Yavuz^{1,2}

DISCLAIMER: This Technical Guidance Note should not be reported as representing the views of the IMF. The views expressed in this paper are those of the authors and do not necessarily represent the views of the IMF, its Executive Board, or IMF management.

JEL Classification Numbers: H63, H1, H12

Keywords: Business continuity planning, business impact analysis, operational risk management

Author's E-Mail Address: ian@storkeyandco.com, hknyvz@gmail.com, ebalibek@imf.org

Publication orders may be placed online, by fax, or through the mail:
International Monetary Fund, Publication Services
P.O. Box 92780, Washington, DC 20090, U.S.A.
Tel. (202) 623-7430 Fax: (202) 623-7201
E-mail: publications@imf.org
www.imfbookstore.org
www.elibrary.imf.org

¹ Emre Balibek is a Senior Economist at the Fiscal Affairs Department, IMF. Ian Storkey and H. Hakan Yavuz are independent consultants.

² This note has benefitted from contributions and comments from Cristina Casalinho, Chairman of the Board of Directors of the Portuguese Treasury and Debt Management Agency (IGCP), David Duarte (IGCP), Juan Luis Díez Gibson (Spanish Embassy at Bern), Andre Proite (the World Bank), Richard Allen, Alok Kumar Verma, Sandeep Saxena, Yasemin Hurcan, Peter Lindner, Hassan Adan, and Tee Koon Hui (IMF).

CONTENTS

I. Introduction	5
II. BCP within an Operational Risk Management Framework	7
III. The Evolving Nature of Threats and Solutions for Cash and Debt Management	8
IV. A Practical Approach to Developing a Business Continuity Plan	12
V. Conclusion	26
Annexes	
Annex I. BCP Template	28
Annex II. Business Impact Analysis Methodology	33
Annex III. Process Analysis Template/Example	38
Annex IV. Incident Management Team	41
Annex V. Pocket Card	42
Annex VI. Scenario and Simulated Live Tests	44
References	47

ACRONYMS

ANAO	Australian National Audit Office
AOFM	Australian Office of Financial Management
BCM	Business Continuity Management
BCP	Business Continuity Plan
BIA	Business Impact Analysis
BNM	Bank Negara Malaysia
BPA	Business Process Analysis
CAT	Catastrophe (Bonds)
COVID-19	Corona Virus Disease
DeMPA	Debt Management Performance Assessment
DRFI	Disaster Risk Financing and Insurance
DRP	Disaster Recovery Plan
FEMA	Federal Emergency Management Agency
ICT	Information and Communication Technology
IFMIS	Integrated Financial Management Information System
IGCP	Agência de Gestão da Tesouraria e da Dívida Pública (Portuguese Treasury and Debt Management Agency)
IMF	International Monetary Fund
IMT	Incident Management Team
ISO	International Standards Organization
IT	Information Technology
MoF	Ministry of Finance
MTPD	Maximum Tolerable Period of Disruption
PC	Personal Computer
RTO	Recovery Time Objective
SaaS	Software-as-a-Service
SCDIs	State-Contingent Debt Instruments for Sovereigns
STP	Straight-through-Processing
TNM	Technical Note and Manual
VPN	Virtual Private Network
WPDM	Working Party on Public Debt Management (OECD)

I. INTRODUCTION

Government treasuries execute cash and debt management functions that are critical for the delivery of government services and functioning of the financial system. The treasury's role¹ includes planning and execution of cash payments to government institutions and raising debt as necessary to meet funding needs, which then enable the government to execute its budget. In fulfilling its roles, the treasury operates in close relation with the financial sector. Disruptions in payment processes, including debt service and cash transfers, can have significant consequences for governments' service delivery and financial markets and can have a negative fiscal and/or reputational impact. Thus, it is critical that cash and debt management operations are resilient to external disruptions, ranging from information and communication technology (ICT) system outages to natural disasters.

Over the last decade, the landscape faced by treasuries has evolved significantly resulting in new threats to business continuity. Some of this has arisen through the evolution of cash and debt management practices such as acceleration of digitalization, including increasing use of digital signatures and automation of processes. These, in turn, have created additional threats (such as cyber-attacks) and unintended ICT disruptions. Changes have also arisen from external factors, including more frequent and severe natural disasters brought about by climate change and, more recently, the COVID-19 pandemic.

Many modern treasuries have business continuity and disaster recovery plans to ensure their core business operations are maintained and losses arising from any business disruption are limited. These plans typically assume a number of scenarios that can disrupt business processes and include measures that can be activated when needed. Scenarios covered in a business continuity and disaster recovery plan (referred to as BCP hereinafter) range from infrastructure and technology failures, to accounting for possible disruptions in computer systems, power, and telecommunications, to natural disasters, such as earthquakes, severe flooding, hurricanes or cyclones that may affect the treasury's premises, data and physical records. Most treasuries now maintain data back-up centers or even secondary (or satellite) sites away from their primary premises, which can be employed immediately should there be a disruption that affects physical infrastructure.

For both advanced economies and developing countries, the COVID-19 pandemic has reinforced the importance of business continuity planning for cash and debt management. Governments around the world announced policy responses to mitigate the socio-economic impact of the pandemic. Implementation of the fiscal policy measures required government treasuries to continue their cash and debt management operations effectively despite their staff having to work remotely and/or in shifts. Treasuries had to meet additional liquidity requirements while putting in place their own administrative measures for continuation of their business processes under the working conditions imposed by the pandemic.

¹ The organization and functions of a government treasury vary considerably across countries. Accordingly, the cash and debt management functions can be fulfilled by a combination of various units such as Debt Management Office, Debt Management Unit, Cash Management Unit, Accountant General and any other country specific entity. In this note, in order to cater for these different practices, "treasury" refers to the government unit(s) that execute government cash and debt management functions, including management of government bank accounts, execution of payment requests or cash transfers to public entities, cash flow planning, and raising and servicing government debt (refer to Figures 2 and 3).

The precedents set by COVID-19 pandemic require some revisions to business continuity planning to maintain operational resilience. While most advanced economies do have a comprehensive BCP, very few (only Colombia, Ireland, Japan and Switzerland among all OECD countries) have included a pandemic as a risk factor.² Existing BCPs are largely focused on protecting businesses from system failures and data losses. There is often less focus on personnel and non-system related business activities. Also, the pandemic has highlighted the shortfall of existing business continuity planning which is geared towards shorter disruptions and do not cover the challenges of prolonged work from home. This is prompting treasuries to rethink their BCP threats and solutions regarding cash and debt management operations.

For developing countries, preparing a BCP still remains a practical challenge. Findings of the Debt Management Performance Assessments (DeMPA) suggest that many low-income and developing countries have not yet developed a comprehensive BCP that covers critical processes in cash and debt management functions (the World Bank 2020). Nkhata (2017) finds that, out of twelve countries in southern Africa, only one has a BCP that qualifies to meet the minimum DeMPA requirements. Challenges potentially include gaps in identification and documentation of critical processes, execution of business impact analysis, resource planning and coordination with partners that support the processes (such as the central bank).

The objectives of this note are twofold: Firstly, building on Storkey (2011), it discusses evolving challenges and solutions to business continuity planning, implied by technological advances and emerging threats over the last decade. In doing so, it complements the broader discussion on rethinking operational resilience and business continuity planning in the financial sector, bringing in the perspective of government treasury management.³ Secondly, it develops and presents a simplified and practical approach to developing a BCP for cash and debt management, as the resources that can be dedicated for this exercise are scarce and applying a simpler approach can save resources significantly. The note presents templates that can easily be adapted by treasuries to draft and implement their BCPs with a focus on cash and debt management. The approach can be extended to cover other treasury functions. For cash and debt management units with very small number of staff and which rely on support services from other agencies of government, the same ideas can be applied to develop the BCP within a wider context (such a ministry wide BCP).

² See OECD (2020a, 2021) for a discussion on BCP practices in OECD countries.

³ See BIS (2021a, 2021b) for discussions by the Basel Committee for Banking Supervision on the changing landscape for operational risks and principles for operational resilience in the banking sector, and Brondolo et al (2020) for a discussion on a BCP for an epidemic in tax administrations.

II. BCP WITHIN AN OPERATIONAL RISK MANAGEMENT FRAMEWORK

Cash and debt management operations are part of the “transactional” functions of a ministry of finance (MoF). These functions, by their nature, are exposed to a more complex set of operational risks as compared to policy or regulatory functions of the ministry. Operational risk refers to “the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events” and has typically been a major concern for institutions and agencies engaged in financial transactions, including government treasuries.⁴

Business continuity planning is a component of the wider framework for operational risk management (ORM). An ORM framework will assess the full range of threats to cash and debt management functions and set out the principles of how operational risks are to be identified, assessed, monitored, and controlled or mitigated. Operational resilience comes from tackling the likelihood of operational risks as well as the consequences of disruptive events.

Internal controls are a key element of mitigating operational risks. Treasuries should have internal controls and procedures to identify vulnerabilities, reduce the likelihood of risks occurring and their impact when realized. Development of an ORM framework falls under the responsibility of the risk management unit within the treasury often in coordination with internal control and/or audit units. The latter functions regularly assess the effectiveness of the internal control framework and ensure compliance. Treasuries should periodically review their ORM framework and adjust their risk limitation and control strategies in the context of the government’s overall risk management strategy and objectives.

Business continuity planning concerns managing the impact on critical business processes of residual risks, i.e. the risk that remains after mitigating controls are implemented. Business continuity planning typically focuses on “high-impact” risks and on the critical functions and activities of the treasury, and assists in preventing, preparing for, responding to, managing, and recovering from the impacts of an incident or disruptive event to ensure operational resilience and limit losses. An effective business continuity planning framework builds on analysis of potential impact of risks on business processes and includes risk mitigation and recovery strategies as well as testing, training and communication and crisis management programs. Frequently, BCP for cash and debt management will need to comply with business continuity directives set by the ministry of finance and external authorities. For example, some countries have set business continuity policies and guidelines for all government agencies to follow⁵ and other countries have a national plan to cover a pandemic or national emergency.⁶

⁴ For more information on operational risk as applied to government cash and debt management, refer to Magnusson et al (2010).

⁵ ANAO (2014), Government of Canada (2013), and Government of France (2013).

⁶ Australian Government Department of Health (2019), Pan-Canadian Public Health Network (2018), New Zealand Ministry of Health (2017), New Zealand Government (2015), and United Kingdom Department of Health (2012).

III. THE EVOLVING NATURE OF THREATS AND SOLUTIONS FOR CASH AND DEBT MANAGEMENT

While COVID-19 presented a major challenge to cash and debt management operations, few existing BCPs made provision for such an incident. Storkey (2011) cited a pandemic as one of the potential incidents but did not incorporate a global pandemic of the nature experienced throughout much of 2020. And while some treasuries have included the outbreak of a pandemic in their BCP,⁷ they did not generally foresee a pro-longed period during which the usual ways of doing business would need to change and traditional solutions would not be applicable (Box 1).⁸ Moreover, treasuries did not foresee that the pandemic would last for more than a year and potentially much longer given the time that will be needed to inoculate the global population.

Box 1. Operational Responses to COVID-19

Many treasuries took measures to prevent the spread of the pandemic and have continued with this policy in 2020 starting from March 2020. Work-at-home measures were complemented with special ICT arrangements as set out in Box 4. Where there has been a need or it has been possible for critical staff to return to the work environment, the introduction of shifts to reduce the number of employees on-site has ensured the treasury meets social distancing guidelines and limits the numbers at meetings and social gatherings. Government directives have dictated what policies or guidelines treasuries have had to follow including maintain a contact tracing record (electronic or physical recording), wearing of masks or personal protective equipment, hand washing, regular cleaning of the workplace, and virus testing should the need arise. In the case of staff that have contracted or been in close contact with someone that has contracted COVID-19, they will have had an obligation to quarantine in accordance with government regulations or guidelines. Three country examples are provided below:

Uganda: In March 2020, the Ministry of Finance, Planning and Economic Development instituted strict institutional adherence to Standard Operating Procedures issued by the Ministry of Health. All staff who had not yet undergone a COVID-19 test were advised to stay at home. Meanwhile, the ministry continued the workforce-scale-down policy for critical staff, minimized contact meetings, maintained safety protocols, undertook regular disinfection of office premises and surroundings, and worked closely with partners and Ministry of Health to mitigate the spread of COVID-19.¹

Portugal: The Portuguese Treasury and Debt Management Agency (IGCP) has been managing different personal situations to ensure employees' safety and well-being. For example, they found new ways for staff to keep in touch and for the treasury to support the mental well-being of staff, since while some were comfortable with more "independence," others felt lost and struggled to

⁷ For example, the Australian Office of Financial Management (AOFM) included a statement in their annual report up until 2015-16, "The AOFM has a comprehensive business continuity plan to ensure that its critical functions can continue in the event of a major disruption or the outbreak of a pandemic" (AOFM, 2016). This was subsequently replaced by compliance with the Australian Health Management Plan for Pandemic Influenza, originally published in 2014 and updated in 2019.

⁸ A survey among financial institutions by the Financial Services Information Sharing and Analysis Center highlighted that, in 45% of cases, staff work from home overwhelmed virtual desktop infrastructure (VDI)/VPN processes. In one third of cases, business continuity IT plans were not prepared for a long-term at-home work force (BIS, 2021c).

engage remotely with day-to-day tasks. Training was maintained throughout the year but performed remotely whenever possible. New hiring was not cancelled but slightly postponed and was done in suboptimal conditions through remote interviews. In March 2020, due to the increase in cases and in order to guarantee operations of critical units, key staff were ordered to start working in shifts of two weeks. After the necessary ICT arrangements, non-crucial staff started working remotely. In June, with the containment of new infections and in an attempt to regain some normality, all staff started working in the office in shifts of two weeks. However, in October, following a further increase in cases, non-crucial staff returned to complete remote work with less than 10 percent of staff working on-site.²

USA: The Treasury was confident in its ability to perform its financing functions but there was apprehension about market participants and their ability. Compounding matters were the broader concerns about the functioning of financial markets as the public health crisis spilled over. Treasury tested extensively in advance of working from home and implemented new communications practices among staff to ensure all mission critical functions could be accomplished remotely through “work-from-home”. Outreach to dealers and buy-side Treasury market participants, both regarding operational resiliency and market conditions, was extensive in the early days and continued in later phases albeit at a less intense pace. The ability for market participants to transition all functions, even back-office, to remote staff has worked remarkably well. The push toward more straight-through-processing over the years was a significant factor in ensuring smooth operations and reduced errors. Efforts by Treasury to increase transparency and reduce uncertainty have also been helpful to market participants.²

1. Uganda Ministry of Finance, Planning and Economic Development (2020).

2. OECD (2020b).

The pandemic revealed that many cash and debt management functions can be conducted via remote working arrangements, provided the necessary digital infrastructure is created. In response to the pandemic countries with strong digital infrastructure and widespread internet services swiftly adopted remote working arrangements and several other practices (as discussed in the next section). Such practices revealed the potential for process improvement via increased digitization and optimization of the processes which require use of physical resources, such as paper and physical media, and highlighted the importance of supporting broader digitalization efforts by governments.⁹ They also demonstrated less dependency on physical infrastructure and a reduced need for an alternative business site(s) for relocation following an incident or disruption. Therefore, reviewing and improving the BCPs, which currently depend on data backups and alternative work sites, in line with the developments in ICT infrastructure would be an important step for increasing the efficiency and effectiveness of these plans. In the new setting, if critical functions can be resumed via tele-working, going to the alternate site might not be the best option under several scenarios.

Digitalization and ICT solutions do not come without risks, however, and appropriate cybersecurity measures should be put in place. Attacks on ICT systems have been rising globally over the last two decades and financial services are typically the most targeted sector (Adelmann et al, 2020). Global

⁹ The additional security provided through a virtual private network (VPN) with encryption together with tele-conferencing platforms for communication across the treasury may provide the necessary confidence to senior management and the auditors to enable work from home as an option for treasury's operations.

COVID-19-related attacks grew to more than 200,000 per week in late April 2020 and stayed above 120,000 till mid-June 2020 (Check Point Research, 2020). Government units engaged in financial activities are also exposed to cyber risks¹⁰ and have been the victims of attacks (see Box 2). Working remotely for long periods increases the vulnerability to cyber-attacks, which can be conducted at a relatively low cost with the evolution of hacking tools. For treasuries that have been introducing technology for issuing government securities or making cash transfers directly to individuals,¹¹ there is an increased requirement to protect the privacy of personal information provided by individuals when using such technology. While not all cyber-risks lead to business disruptions, ICT related business continuity risks can amplify the exposure to cyber-risks. Therefore, the measures implemented for business continuity should be able to defend, respond, and recover against unauthorized access to ICT systems, communication platforms, and other digital applications.

Box 2. Cyber Risks for Public Financial Institutions

In February 2016, the Central Bank of Bangladesh was attacked via a series of unauthorized transactions made on an official computer.¹ Attackers tried to deliver the money in various accounts in different countries using the SWIFT system. The attack was started on Thursday, February 4 and continued on Friday, February 5 (a public holiday in Bangladesh, but a working day in the United States and Europe) by sending 35 payment instructions worth of US\$951 million to the Federal Reserve Bank of New York. The first 5 transactions were completed, but the remaining 30 were blocked partly because of the failures made by the attackers (such as a spelling mistake in the payment transaction, which prevented the automatic system from completing the transaction.² However, between February 5 to 9, attackers were able to withdraw US\$81 million in total under fictitious identities.

In March 2018, a similar attack was made on the Central Bank of Malaysia. The attackers attempted unauthorized fund transfers using falsified SWIFT messages. In its press release Bank Negara Malaysia (BNM) stated all unauthorized transactions were stopped through prompt action in strong collaboration with SWIFT, other central banks and financial institutions.³ BNM did not experience any financial loss in this incident. There was also no disruption to other payment and settlement systems that BNM operates.

In March 2020, Norfund—Norwegian state-owned investment fund for developing countries—was exposed to a serious case of fraud of US\$10 million through a data breach. Defrauders manipulated and falsified information exchange between Norfund and a borrowing institution over time in a way that was realistic in structure, content and use of language.⁴ As a result of this extensive manipulation of communication, the defrauders were successful in diverting funds to an account not belonging to the intended recipient. The fraud took place on March 16 but discovered on April 30 when the scammers initiated a new fraud attempt.

These cyber risk incidents in many varieties aimed at exploiting vulnerabilities in international bank account monitoring, network and physical security, credentials and weekend protocols.⁵ These examples are particularly important for government cash and debt management functions, since they are now highly integrated to banking infrastructure through their FMIS, which enables

¹⁰ Cyber risk refers to “the combination of the probability of cyber incidents occurring and their impact” Financial Stability Board (2018).

¹¹ Two examples are M-Akiba in Kenya and BONDS.PH in the Philippines where bonds can be purchased through an application on mobile phones.

electronic funds transfers. The incidents underlined the importance of establishing a cyber-security governance and cyber security culture, maintaining an effective vulnerability management program and developing an incident response plan.

1. Hämäläinen et al. (2018).
2. The Guardian (2016).
3. Bank Negara Malaysia (2018).
4. Norfund (2020).
5. Allison (2019).

Many sovereign treasuries have agreements with the central bank and private banks to act as a fiscal agent for the treasury. As these agents are key counterparties in conducting cash and debt management operations, coordinated efforts are needed to ensure using ICT solutions and implementing cyber security measures in a harmonized way. Therefore, the financial and technological connections between cash and debt management and the banking sector should be incorporated into business continuity policies to contain the impact of a possible disruption in one of the key counterparties and to strengthen the resilience of cash and debt management operations.

For major threats, there is a need to coordinate on a national or federal level. In the case of COVID-19, virtually all countries imposed some form of lockdown, and governments issued directives and guidelines on what was acceptable for all businesses, including treasuries. As a result, the BCP had to comply with such directives and guidelines (see Box 1). The BCPs frequently also had to comply with work-at-home directives.

IV. A PRACTICAL APPROACH TO DEVELOPING A BUSINESS CONTINUITY PLAN

Overview of Business Continuity Planning: Rethinking the Conventional Steps

Developing a BCP typically follows a step-by-step approach.¹² The conventional approach starts with a comprehensive Business Process Analysis (BPA), which is followed by a Business Impact Analysis (BIA), in order to identify and verify the critical functions of the organization. A BPA is a systematic process that identifies and documents the activities and tasks that are performed within an organization. Specifically, BPA captures and maps the functional processes, workflows, activities, personnel expertise, systems, resources, controls, data, and facilities inherent in the execution of a function or requirement. An effectively conducted BPA supports the development of detailed procedures that outlines how an organization accomplishes its mission (FEMA, 2018). The BIA follows the BPA and serves for identifying and evaluating the effects of various threats and their possible impact on the ability of an organization to perform its critical functions. The information collected through the BPA and the BIA is then used to design the relevant risk mitigation techniques to be covered in the BCP. Conventional BCP development steps are presented in Figure 1.

While the undertaking to develop a BCP can provide important insights for better management of processes, some treasuries find the steps to be arduous, particularly when they have limited resources and a heavy work program. Country experiences suggest that documentation efforts for the BPA and BIA often require too much effort for too little value, can become quickly outdated, and are setting time targets that may be unrealistic and unreflective of what would actually happen in a crisis.¹³ Moreover, preparation of process maps, workflows and manuals requires significant time and resources, and particularly for treasuries in developing countries and frontier market economies, there might not be enough resources that can be dedicated to these activities. Accordingly, there is a need to simplify the BCP development process and documentation, to make the task easier and less onerous on cash and debt management resources.

This section lays out a simplified four-step process for developing and maintaining the BCP. The TNM particularly focuses on simplifying the BPA/BIA¹⁴ steps by pre-screening processes and disentangling the components of the BIA (Figure 1). Annex I presents a BCP template along these lines.

Step 1: A Simplified BIA

The BIA identifies the critical functions, reveals an institution's vulnerabilities, and helps determine the cost of undesirable events. While developing a BCP, an institution needs to fully understand its activities, processes, and systems and identify the threats that might have an impact on its operations. The information gathered at this stage both provides an evaluation of the current practices and sets the basis for the allocation of resources (money, people, time, ICT needs) to

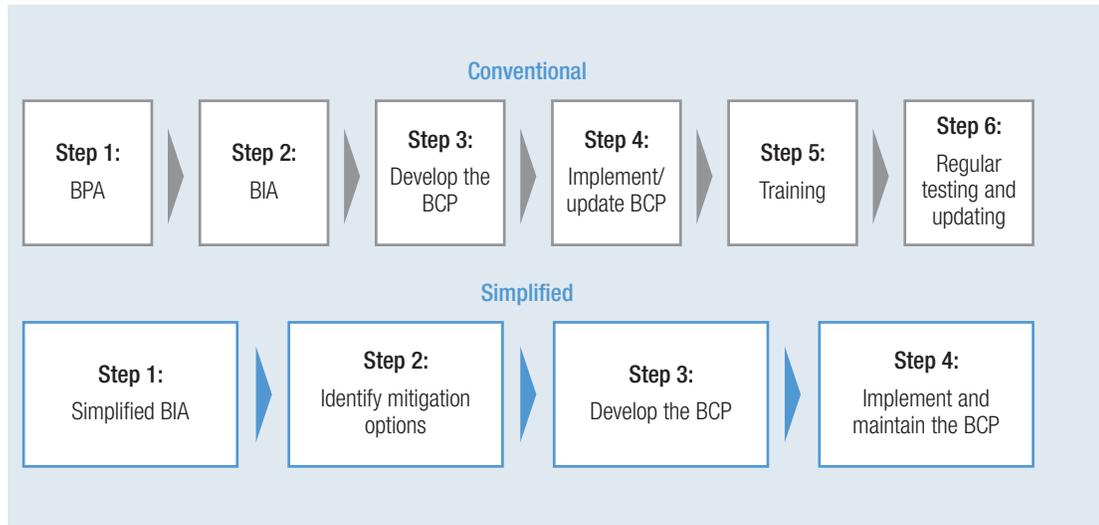
¹² Refer to Storkey (2011) for a six-step process to develop a BCP.

¹³ Refer to Chapter 1 of Lindstedt and Armour (2017).

¹⁴ Refer to Business Process Analysis and Business Impact Analysis User Guide (FEMA, 2019a) and ISO 22301:2019 Business continuity management systems-requirements.

mitigate risks and ensure operational resilience. The components of a typical BIA are discussed in Box 3. This TNM introduces a pre-screening stage to limit the number of processes for which the BIA is done. The BIA is further simplified by reducing the number of risk scenarios under which processes are assessed.

Figure 1. Comparison of Conventional and Simplified BCP Development Steps*



Source: Authors.

* Steps 5-6 of the conventional approach is equivalent of Step 4 of the simplified approach.

Box 3. The Components of Business Impact Analysis

Identification of possible scenarios/threats

BIA should identify the threats that might jeopardize the operations of an institution. Risk scenarios define the situations under which business continuity of processes might be impacted. There can be numerous possible scenarios,¹ and identification of a comprehensive set of scenarios might be a challenging task. Scenarios should not only take into account what has happened before, but what can potentially happen in the future.

Assessing the likelihood of possible scenarios/threats

A BIA should also assess the likelihood of possible scenarios. Scenario probabilities can be calculated by using statistical methods if data are available. For instance, the operational risk management information system used by the Turkish Treasury collects and records data as the incidents are reported by the users.² However, having such data is quite unlikely in the absence of an operational risk management information system. Also, data pertaining to rare events needs to be sourced over long periods at a global scale. Thus, alternatively, this analysis could be done qualitatively by the dedicated team via meetings and workshops assessing the likelihood of scenarios relative to each other.

Evaluation of impacts of scenarios/threats on processes

In terms of evaluating the impact, not all operational risks will be of equal importance for the treasury as this will be specific to the environment and the risks faced. For cash and debt management, reputational impact, reporting impact and the impact on operations need to be considered within the analysis.³ The treasury should evaluate the scenarios' impact on each of these categories and undertake an assessment considering all of the three impact categories.

Time criticality analysis of disruptions

The BIA should include an analysis of the time-criticality of each process as well. Time criticality refers to the recovery of treasury's most critical activities, processes and systems in terms of the time period (minutes, hours or days) in order to maintain essential/critical operations. For example, there could be end-of-day activities or processes that may need to be completed before a cut-off at the end-of-the-day for which time criticality increases as the deadline approaches, such as submitting payments to the central bank for processing through the overnight banking system. Another example is the cut-off and processing times during the auction of government securities where there could be several critical times throughout the auction and settlement process. A table of essential/critical activities should be developed and maintained by the treasury that sets out the time-period when each essential/critical activity is required to be fully operational.

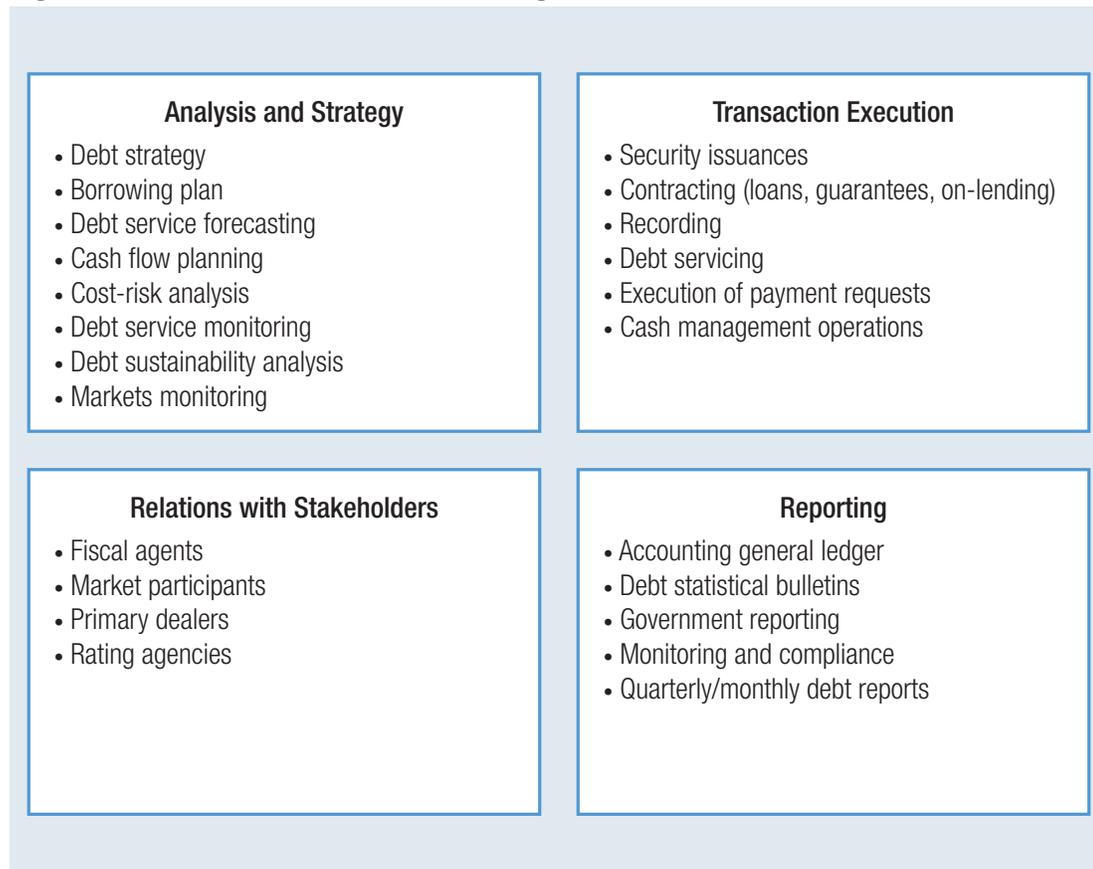
The analysts need to assess how long a process can be halted or disrupted without major consequences if one of the scenarios happens. "Maximum Tolerable Period of Disruption"⁴ or MTPD, is the maximum allowable time that the organization's key products or services is made unavailable or cannot be delivered before its impact is deemed as unacceptable.⁵ Similarly, Organization for Standardization (ISO) defines MTPD as the time frame within which the impacts of not resuming activities would become unacceptable to the organization.⁶ Just because a process is deemed important in terms of impact and likelihood, this doesn't mean it needs to be recovered immediately or kept resilient. Likewise, processes which have low impact or scenarios with low likelihood might also have adverse impacts if halted for a long time or at certain dates/ periods. Thus, assessment of MTPD and identification of time criticality are vital to make informed decisions about how much to invest for making each process more resilient or recoverable swiftly.

1. Storkey (2011).
2. Turkey Ministry of Treasury and Finance (2014).
3. Examples of the impact on cash and debt management were set out in Table 3 Mexico Impact Criteria Framework in Storkey (2011).
4. Also known as Maximum Acceptable Outage (MAO) as documented in Brondolo et al. (2020).
5. BCM Institute (2020).
6. ISO 22301 (2019).

Pre-screening Business Processes

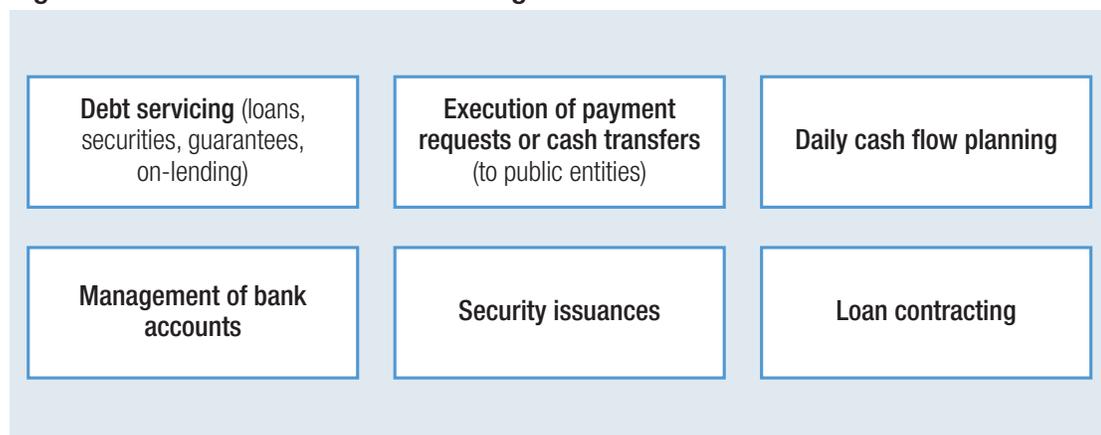
To simplify the conventional steps of BCP development, treasuries can focus on a select set of processes. Pre-screening of processes can help identify a process to be nominated for more detailed impact analysis and reduce the burden of lengthy documentation of all processes (as it would be with the conventional approach). There are many common cash and debt management functions performed similarly across countries (Figure 2), and country experiences suggest that certain processes are more critical than others. Critical processes would typically include those shown in Figure 3 but should be complemented with country-specific critical tasks.

Figure 2. Common Cash and Debt Management Functions



Source: Authors.

Figure 3. Critical Cash and Debt Management Processes



Source: Authors.

Combining the Components of BIA

The processes that are identified in the pre-screening step can now be subject to more detailed (but still simplified) analysis to confirm their criticality under risk scenarios. The conventional BIA approach analyzes numerous specific incidents/scenarios separately and assess their impacts

Table 1. Main Scenarios¹

Scenario Theme	Scenarios Based on Duration of Impact		
	Intraday (a few hours)	Short-term (1–5 days)	Medium-term (> week)
S1 Physical Infrastructure Inaccessible	S1.1 Ex: minor events leading to evacuation of the building	S1.2 Ex: local fire, flood etc.	S1.3 Ex: earthquake/major climate event, closure of offices due to pandemic etc.
S2 ICT System Failure (main system)	S2.1 Ex: outages	S2.2 Ex: cyber-attacks, physical impact of an event on hardware	S2.3 Ex: prolonged hardware or system failure with complete reinstall, rebuild and re-entry of debt data
S3 Staff Unavailability	S3.1 Ex: impact to authorized signatories	S3.2 Ex: Terror attacks	S3.3 Ex: epidemic, pandemic reducing staff availability (contagion)
S4 Key Counterparty/ Service Provider Failure	S4.1 Ex: outages in third party services	S4.2 Ex: extended interruptions in third party services	S4.3 Ex: service provider ceasing to provide services

Source: Authors.

¹This is not an exhaustive list and should be amended based on country circumstances.

on processes. However, assessing the impact and likelihood of each particular incident/scenario is exhaustive. For instance, a power failure, fire, or a gas leak might all lead to unavailability of physical infrastructure for several hours i.e. the ultimate impact on processes is similar even though the root cause can be different.

In order to simplify the BIA, risk scenarios can be grouped in terms of their impacts and thus the total number of scenarios can be decreased significantly. The duration of potential impact of scenarios can be assessed under 3 basic time frames: Intraday, short-term (1-5 days) and more than a week. A template for main scenarios is provided in Annex II. Table 1 provides four main possible scenario themes and a total of 12 scenarios based on duration of impact based on international real-life incidents. This structure enables the practitioners to evaluate numerous possible scenarios under main headings.

Once the scenario themes are identified and categorized, their likelihoods, their impact, and time criticality of critical processes should be assessed. Countries can use a “combined risk score” where these three factors are aggregated in the assessment. In this approach, the likelihoods of scenarios, their impact on critical processes, and time criticality¹⁵ are each assessed separately over a three-point scale (low-medium-high). These assessments are then unified to form a “combined risk score” – two “high” scores in a “scenario/process combination” qualifies this combination for inclusion in the BCP. Table 2 provides an example, for the “Debt Servicing” process.¹⁶ Annex II provides further guidance, including the possible scales and definitions that can be used for such assessments, including time criticality analysis.

The processes that are confirmed to be critical in the BIA should be included in the BCP. The example in Table 2 confirms the “criticality” of the debt service process since it is time critical (i.e. cannot be delayed over a certain period without reputational or financial consequences) and/or can

¹⁵ Time criticality analysis compares the “Maximum Tolerable Period of Disruption” for the process with the duration of the scenario under consideration – See Box 3 for definitions and Annex II for more a detailed discussion.

¹⁶ It is possible to increase the degree of granularity in this analysis. The debt servicing process has several steps from start to finish and can be divided into sub-processes which can be assessed separately (see Annex II).

Table 2. Example for Assessing Combined Risk Scores

Processes		Scenarios											
		S1			S2			S3			S4		
		S1.1	S1.2	S1.3	S2.1	S2.2	S2.3	S3.1	S3.2	S3.3	S4.1	S4.2	S4.3
Debt Servicing	<i>Impact of Scenario on the Process</i>	High	Medium	High	High	Low	Low						
	<i>Likelihood of the Scenario</i>	Medium	Low	Low	Medium	High	Low	High	Low	Low	Low	Low	Low
	<i>Time Criticality of the Process</i>	High											
	Combined Risk Score	HiMeHi	HiLoHi	HiLoHi	HiMeHi	HiHiHi	HiLoHi	HiHiHi	MeLoHi	HiLoHi	HiLoHi	LoLoHi	LoLoHi

Source: Authors.

be impacted by various “high impact” scenarios.¹⁷ In particular, the scenarios highlighted should be considered and risk mitigation options should be documented in the BCP. The analysis (through the high time criticality scores) also indicates the BCP should include rapid recovery procedures for the debt servicing process.

Critical processes should be further analyzed in terms of input/outputs, critical resources (staff, ICT, infrastructure etc.) and associated risks at particular stages. This analysis helps develop written guidelines of the BCP and help staff to perform duties in emergency situations. A template for a process workflow (including the workflow of generic debt servicing functions) and its modified version under BCP are provided in Annex III. The information gathered in this analysis establishes the foundation for evaluating the risk mitigation strategies which are discussed in Step 2. These mitigation options and recovery procedures can be scenario-specific. Nevertheless, in some cases arrangements for a shorter disruption could also work for a longer disruption. For example, arrangements for processing debt service remotely could work both when the building is evacuated and when staff has to work from home during a pandemic.

Step 2: Identifying Mitigation Options

There are typically four categories of options that are used to mitigate the risk of disruption (Storkey, 2011), namely:

- **Prevention or avoidance**, where the probability of an event occurring is reduced or eliminated by putting in place systems and procedures to minimize or where possible eliminate the risk of disruption.
- **Transference**, where risks are passed to third parties by taking out insurance and/or reinsurance, outsourcing or devolving critical activities to third parties, and establishing facilities to provide financial resources in the event of a major incident.¹⁸
- **Containment**, where the potential impact of an event occurring is limited in the early stages using controls or other techniques and putting in place escalation procedures including an Incident Management Team (IMT) to manage major incidents.

¹⁷ This example is for illustrative purposes only and the combined risk scores for each scenario will be specific to the environment and risks faced by the treasury.

¹⁸ An example is State-Contingent Debt Instruments for Sovereigns (SCDIs) which is a countercyclical and risk-sharing tool as covered in International Monetary Fund (2017).

- **Acceptance and recovery**, where an event or disruption might well occur, but cash and debt management operations can be resumed and continued successfully using the disaster recovery plan.

New technologies and concepts have enabled practical solutions (see Box 4) to implement these mitigation options. Some examples include:

- **Teleworking:** making use of technologies to work from home or a remote location that enable secure and encrypted internet connections and channels of communication using tele-conferencing platforms along with cloud storage to protect sensitive data. This reduces the need for an alternate operations site where cash and debt management staff would relocate should their main office premises be unavailable or inaccessible. Telework arrangements should be supported by regulations that provide a statutory and operational framework.¹⁹ An efficient telework framework should rely on a safe and secure manner ICT infrastructure, as exemplified during the COVID-19 pandemic.

Box 4. ICT Solutions for Business Continuity under Teleworking

- **Brazil:** Debt management operations relied on a virtual private network (VPN) with an external dedicated server and backup that was set up a year before the pandemic and tested in February 2020. Issuance and debt service functions were executed remotely, using web-access to central securities depositories and web-based version of Bloomberg services. Press reports and meeting were held virtually.¹
- **Korea:** Working with the Ministry of Economy and Finance, the Korea Public Finance Information Services (KPFIS), a public institution that manages and operates the dBrain system, i.e. the IFMIS, used the Government VPN system to allow users to handle administrative affairs like an office as long as the user has an internet connection at home or abroad. The authorities used cloud-based work data storage, established infrastructure for creating and editing documents remotely, strengthened and expanded chat services, and increased the use of portal announcements (notices and bulletins) via dBrain (digital budget accounting system).²
- **Portugal:** The Portuguese Treasury and Debt Management Agency, IGCP, set up VPN access to systems and acquired licenses to hold virtual meetings. The firewall and network infrastructure were updated. New hardware requirements (laptops, access points, webcams, microphones) were gradually met allowing all staff remote access to government systems.³
- **Turkey:** The Ministry of Treasury and Finance set up VPN access and remote desktop connections (for critical staff in the first place, then extended to all staff), established safe internet connection and put professional webcams/microphones to numerous meeting rooms for virtual meetings.
- **USA:** The US Treasury maintained and tested “hot” fail-over operational sites.⁴ The authorities increased VPN capacity and bandwidth to deal with increased volume of users on VPN

¹⁹ An example is the “Telework Enhancement Act of 2010” in USA, which requires executive agencies to incorporate telework into their “continuity of operations” plans and employees and managers to complete interactive telework training.

networks and to minimize latency issues and embraced a number of new virtual meeting technologies.

In order to reap the benefits of the ICT solutions without increasing their risk exposure, treasuries need to implement strong security measures. Experience suggests cyber risks are better mitigated by containing the threat at its source. In general, the authorities should identify critical information assets and infrastructure upon which they depend and have a documented ICT policy. In particular, the following measures are recommended to support the cybersecurity of remote work.⁵

- Authorities should quickly and effectively implement good practices and international technical standards applicable for secure remote working (e.g. NIST 800-46 Rev 2, BSI IT-Grundschutz Compendium, COBIT 2019, ISO 27000 series).
- Remote access services and user profiles should be only activated when required.
- Cloud usage should be based on detailed risk assessments.
- Teleconferences should be run on vetted platforms and protected from unauthorized access.
- Additional awareness campaigns on cybersecurity should be launched for all employees.
- Robust controls over configurations at both ends of the remote connection should be implemented to prevent potential malicious use.
- Entities should implement additional security controls for critical functions that are normally not allowed to work remotely.
- Supervisors should reinforce the message that remote work increases cybersecurity risk, which must be addressed with strong controls.

1. Proite et al (2020).

2. KPFIS (2020).

3. OECD (2020b).

4. "Fail-over" refers to switching to a stand-by system upon failure of the primary system. A "hot" site is a near duplicate of the original site of the organization, with full computer systems and complete backups of data. A "cold" site is a backup facility with little or no hardware equipment installed.

5. Adelman and Gaidosh (2020).

- **Devolution:** setting up under a statutory delegation, executive order or power of attorney to transfer responsibilities from the primary staff of the treasury to other designated staff, alternate location, sub-ordinate agency or third party such as the central bank or other government agency the authority to undertake activities until the primary staff are able to resume these activities following a major incident. Devolution would be activated through a significant incident such as the government's declaration of a state of emergency. For these instances, the authority should be very tightly defined with clear assignment of functions and time-periods to ensure that strong governance is maintained and there is no risk of fraud or corruption. Devolution is a relatively complex risk mitigation strategy as discussed in Box 5. A devolution plan can be prepared as a separate document to the BCP to provide the direction and guidance to the treasury that operations continue during any emergency with minimal disruption to essential functions.²⁰

²⁰ A devolution plan published by the US Federal Emergency Management Agency (FEMA) can be a useful template (FEMA, 2019b).

Box 5. Devolution

Devolution involves the transference of a critical operation to another party which could be permanent or for a limited period under a statutory delegation, executive order or power of attorney in order that this operation can continue following an incident without the involvement of the primary staff responsible for cash and debt management operations. Devolution can be more suitable for organizations with field and regional offices. The central bank is a main partner in cash and debt management as it is the fiscal agent and holder of main accounts, and therefore a natural candidate for devolution of cash and debt management functions.

When using devolution as a risk mitigation option, the treasury should prepare a training program for the staff of the devolution partner on critical functions and ensure that they have access to necessary ICT structure. Triggers, roles and responsibilities should be clearly defined. Triggers to initiate the devolution option can include active and passive triggers. Active triggers include a deliberate decision by the management of the treasury, while passive triggers define conditions under which the partner organization assumes responsibilities. In many countries, devolution can necessitate amendments to finance and treasury legislation or regulations. These amendments can include delegations to cover activation and authorizations, including authorized personnel or signatories with procedures established and approved for all third parties. Devolution examples can include:

Domestic securities issuance: assigning the authority to the central bank to conduct the auction of government treasury bills or bonds without the need for the treasury to be directly involved.

Debt service payments: assigning the authority to the central bank or regional treasury offices to make debt service payments, particularly when the designated signatories and/or payment systems are unavailable when the payment deadline falls due.

The US Treasury conducts regular devolution exercises across the organizations involved in managing the treasury auctions. Plans foresee the devolution of certain activities to other units of the treasury should the primary unit for that task be not available due to a business disruption. While this has not been needed during 2020, plans are in place and are ready to be acted on should significant issues arise (in addition to work-from-home), such as technology failures or an inability to communicate between policymakers and operational staff.¹

1. OECD (2020b)..

- **Straight-through-processing:** making use of treasury and integrated financial management information systems that provide electronic processing from issuance to settlement (referred to as straight-through-processing or STP) with interfaces and connectivity to SWIFT and other payment systems.
- **Software-as-a Service (SaaS):** contracting a third-party software provider to host treasury systems and associated data in order to reduce IT support costs by outsourcing software maintenance and support to the SaaS provider under a subscription arrangement with a monthly or annual fee. Hardware support can also be outsourced (infrastructure-as-a-service). With increased internet speeds and reliability, some treasuries have opted for this approach. For

example, the federal and some state governments in Australia and the central government and local government funding agency in New Zealand are using SaaS for their core treasury debt management system.

- **Data centers:** entering into an arrangement with a third party to host an alternate data center (which can be for the treasury alone, shared with the MoF, or for the whole of government) to enable replication of treasury systems and associated data. The frequency of replication depends on the cash and debt management operations' time criticality. For example, if systems and associated data are required with minutes or even seconds (e.g. active liability management and trading activities where access to real-time data and systems are required), mirroring of the debt management system may be required, but this can be expensive. Most treasuries can operate with less frequent replication (often daily with the transfer of debt data to the data center overnight). Ideally, connections to the alternate data center should be triangulated (through the central bank or another agency of the government) to minimize the risk of single point-to-point failure. Increasing use of cloud storage solutions reduces the need for replication of debt management systems and associated data at an alternate data center.
- **Contingent financial resources:** addressing the increased frequency and severity of natural disasters linked to weather, water and climate-related extremes, and now with the addition of the global pandemic, governments have been looking for putting in place facilities to provide financial resources to cover the additional and unexpected budget costs needed to restore business operations following a disaster. Financial resources available include issuing catastrophe (CAT) bonds, establishing a national catastrophe or contingency fund, or entering into a disaster risk financing and insurance (DRFI) program to provide a ready source of funds to respond immediately in the event of a major local or national disaster. Availability of contingent financing options reduce the time criticality of government auctions.

For the mitigation options to be effective, there will be prerequisites and factors to consider.

Some of these will include incorporating telework into the BCP, upgrading the ICT infrastructure, establishing incident management and back-up teams for activation of the Disaster Recovery Plan (DRP),²¹ installing and implementing tools and systems to identify and contain cyber-attacks, as well as reviewing and updating legal and regulatory frameworks. Particularly, this would be necessary for putting in place any devolution arrangements with orders of succession, delegations of authority, and service level agreements with the central bank and other key third parties. It is also advisable that joint tests are conducted with key third-party providers to ensure that all parties understand their respective roles and can operate following an incident.

Selection of the most effective mitigation strategy depends on several factors such as the scenario, impact, time criticality, budget constraint and availability of the necessary services in the jurisdiction. The preferred option is prevention or avoidance primarily through internal controls and replication of systems and data. If this is deemed difficult or expensive to achieve, some functions or activities can be transferred to third parties to reduce or mitigate the risks. There will be incidents where these two options will be insufficient due to a major incident beyond the control of the treasury. In this case, the option of containment becomes the priority, but if the incident escalates, the IMT will activate the BCP. In the development of the BCP and subsequent training, the mitigation options can be examined by the treasury to determine the principles to be

²¹ Throughout this note, the DRP is integrated into the BCP. The DRP will be activated for major incidents or disruptions that will primarily be required under the “containment” and “acceptance and recovery” mitigation options.

Table 3. Mitigation Strategy Identification Example

Process	Main Scenarios	Mitigation Strategy Options
Debt Servicing	S1 Physical Infrastructure Inaccessible	<ul style="list-style-type: none"> • Activation of <i>DRP</i> • Alternate site • Teleworking • Devolution
	S2 ICT System Failure	<ul style="list-style-type: none"> • Install backup or redundant systems • Alternate data center and replication • Activation of <i>ICT DRP</i> • Devolution • Software-as-a-Service
	S3 Staff Unavailability	<ul style="list-style-type: none"> • Alternate staff • Devolution • Teleworking
	S4 Key Counterparty/Service Provider Failure	<ul style="list-style-type: none"> • Straight-through-processing • Joint-tests

Source: Authors

applied in deciding on the appropriate option(s). If one mitigation option is not available but deemed useful in preventing the majority of incidents, action plans with reasonable timelines could be prepared. Table 3 provides an example for identifying possible mitigation strategies under different scenarios for the select debt servicing process. Depending on the process and scenario, these mitigation options should consider solutions regarding workforce deployment, ICT and use of alternative facilities.

The BPA for the critical processes would be useful for identification of the most effective and suitable mitigation strategies. Country experiences suggest that improvements in the business processes arising from the BPA (such as improved controls, restaffing etc.) can reduce the likelihood of risks and/or their potential impact on the process, and therefore help reduce the cost of mitigation.²²

There may also be a need for some degree of business process reengineering for the mitigation options to be acceptable and workable. For example, the process flows can be different when the BCP is activated, particularly when working from home, as electronic signatories may be necessary rather than physical signatures. This may prompt a move from physical to digital processing (i.e. digitization) with the need not only to change procedures but also to train staff on the digital platforms.

Many governments still rely on manual approval processes to transfer cash or conduct borrowing auctions. Ministers or accountant generals may have to approve electronic fund transfers, heads of borrowing units (or sometimes ministers) might sign off on cut-off yields in government securities auctions. Modern FMIS systems are enabled for setting up automated workflows and approval mechanisms, but these systems may only be accessible from the primary and secondary sites, not through VPN-connections from staff homes.

Decision making, command and approval processes can be reconsidered to enable continuity of operations. For example, some processes that include several ex-ante controls could be simplified when the BCP is activated, replacing some pre-approval requirements with ex-post audits within

²² As an example of the experiences of working from home, IGCP undertook a BPA to initiate an overhaul of its business operations that is likely to result in a review of functions and staffing across IGCP (OECD, 2020b).

a short timeframe. Other manual or electronic workarounds with appropriate safeguards could be established to execute critical control processes. An example of modification of a business process flow through such a review is shown in Annex III.

While some mitigation options can be implemented at minimal cost, there will be a trade-off between the cost of prevention and/or recovery and the recovery period needed by the cash and debt management operations. The cost-recovery time trade-off is usually not linear for some processes as the cost to shorten the recovery time will require a significant investment in ICT systems, training etc. (Storkey, 2011). Therefore, a key element to consider for the cash and debt management is the cost-recovery time trade-off and the justification needed to incur additional budget expenditures to implement the mitigation measures. For example, the cost of establishing and maintaining an alternate site for staff should they need to relocate from their primary premises may not be justified when considering the alternative of a “work from home” arrangement. The latter raises additional ICT security concerns, which can be alleviated through secure and encrypted channels of communication and cloud storage to protect sensitive data.

Step 3: Developing the BCP

Once the business impact analysis has been completed and mitigation options have been identified, the treasury should formulate a plan that addresses those critical incidents. The principles that should be elaborated in the BCP and the questions that should be addressed are:

- **Activation procedures:** how will the BCP be activated, under what conditions, how are staff informed when the BCP is activated (i.e. decision and communication tree structure), and what are the critical activities or functions and resources that are addressed in the BCP?
- **Management:** who is responsible for activating the BCP, who is included in the incident management team, who will be responsible for communication and media liaison, who will coordinate with HR and corporate services, and what training for management is needed to prepare them for the role in the incident management team?
- **Scenario planning:** what is the mitigation option for each critical scenario, how will mitigation policies be implemented, what infrastructure and resources are needed to be in place for each scenario, and how frequently should the scenario be tested?
- **Return to normalcy:** what are the prerequisites for return to normalcy under the different scenarios, how will these be managed, and what should be retained at the alternative locations in preparation for future incidents?

Templates are provided in the Annex to assist with the drafting of the BCP. These include (i) a sample of a simplified BCP template in Annex I; (ii) the outline of the business impact analysis methodology in Annex II; (iii) a process analysis/template in Annex III; and (iv) the potential structure of an incident management team in Annex IV.

Practical experience suggests short guides for staff are most useful as an initial document for reference when business disruptions occur. A “pocket card” can conveniently document the incident response plan to prepare the cash and debt management staff for a timely response to critical incidents and reduce the impact of those incidents on previously identified operations. It also

prepares key personnel to provide an effective response to ensure minimal disruption to operations in the event of emergency. Annex V contains an example of a card that can be kept by cash and debt management staff in a physical or electronic form and contains the type of information needed, including content of an emergency kit and a checklist.

Step 4: Implementing and Maintaining the BCP

Once the BCP has been drafted, measures are required for the plan to be implemented and imbedded into the day-to-day cash and debt management operations:

- **Budget provision:** Preparation of a budget, both upfront and ongoing, that will cover the implementation and maintenance of the BCP. This will also extend to the need to make provision for training and regular testing of the BCP.
- **Acceptance:** Agreement/endorsement from all senior management and business units of the treasury of all elements of the BCP including the budget and the response to the critical incidents for their respective units. It is senior management that has ultimate responsibility for acceptance of the BCP once it is developed and for ongoing maintenance including integration into the day-to-day operations of the treasury.
- **Approval:** High level approval depending on the local regulations and instructions (which may include approval from the minister, vice minister, permanent secretary, director general, or steering committee) and the budget implications.
- **Integration:** Ensure that the BCP is integrated into the day-to-day operations by updating policies and procedures, requiring that business continuity planning is included in future policy changes, establishing a process for keeping the plan current, and for training and regular testing. For treasury, it is particularly important to consider the BCP implications of introducing new instruments and activities or new technologies in order to fully evaluate the business impact and risks should there be an incident or disruption.

For the process of integration to be successful, it will be important to raise awareness across the treasury of the existence of the BCP, why it is important and what the responsibilities of all staff are with maintenance, update and activation of the BCP. This will involve the following activities:

- **Communication:** This involves generating an understanding of the BCP across the treasury and ensuring buy-in of all staff. Workshops should be conducted where the plan is introduced, explain how each business unit needs to take responsibility for the rollout and maintenance across their respective unit, and the role of each individual across the treasury to consider business continuity planning in their day-to-day operations. It will also explain how the communication tree will operate in the case of a significant incident, particularly if it occurs outside normal business hours and when the main office premises are unavailable or inaccessible.
- **Training:** This initially involves the preparation of a training plan, both initial and ongoing for all business units across treasury. The plan can include a training program for the whole of the treasury or for individual business units. It is important that the training includes senior management even though it is acknowledged that their availability may be limited. It is also important to

develop training plans to cover third parties, particularly where devolution of responsibilities is involved. All new recruits should be provided BCP training as soon as possible after joining the treasury.

- **Scenario tests:** This involves conducting in-house classroom style exercises. These scenarios can be based on actual incidents that the cash and debt management staff has had to address in the past along with scenarios that have arisen from the BIA. It is often useful for the scenarios to be constructed in a way that evolves and escalates as is often the case in a real-life situation. This is best illustrated with the sample scenarios provided in Annex VI.
- **Simulated live tests:** This involves conducting exercises with either simulated live simulations or preferably actual live tests of operations at an alternative site.

Scenarios and live tests are critical to identify and address the problems in the BCP. Once the issues identified are addressed, tests provide comfort to the staff responsible for the activity or process but also for senior management to provide the assurance that the treasury could cope in the case of an incident. Moreover, experience from country examples (including Colombia, Mexico and Peru) suggest that the live tests generate interest across the whole of the treasury and create the enthusiasm for staff to participate in subsequent live tests. The experience of the Mexican treasury (TESOFE) in maintaining an alternate operations site (located within Mexico City) which received compliments on their readiness to respond to the earthquake in September 2017 through the successful activation of the BCP.

For debt management operations, tests should ideally include and assess the preparedness of the cash and debt management main counterparts, including the central bank and potential participants in auctions. In the US, for example, on October 24, 2020, an industry-wide testing was conducted to assess and verify the ability of firms, markets and utilities in the securities industry to operate through a crisis using a combination of primary, backup and recovery facilities and backup communications capabilities. As part of the test, a government securities auction was simulated (SIFMA, 2020). Such tests help identify issues that may challenge the ability of financial firms to participate in government auctions under nation-wide disruptions. The US Treasury has in place a requirement that primary dealers maintain and test a geographically dispersed disaster recovery site and also perform functions from remote sites (at home) other than the disaster recovery site. In 2013, after a hurricane that led to business disruptions in financial firms in the New York area, primary dealers were asked to ensure that they had back-up sites outside Manhattan (OECD, 2020b).

V. CONCLUSION

Business disruptions to governments' cash and debt management operations can have spill-over effects on the delivery of government services and on the functioning of financial markets. Delays in government payments can impact timeliness and quality of services provided by government agencies. A government bond auction that fails due to operational risks, for example, an outage in the electronic auction platform or a belated debt service because of interruptions in internal approvals may have financial and/or reputational consequences with possible impact in a nation's financial system.

Treasuries should take measures to safeguard their ability to continue their critical operations under business disruptions. For government treasuries, critical cash and debt management processes comprise cash flow planning, managing bank accounts, cash transfers, and raising and servicing debt. BCPs should aim at building operational resilience for these processes considering the evolving environment for risks.

Business continuity planning should benefit from technological advancements and global experience with managing threats over the last decade. With the arrival of web-enabled systems, reliable internet services, sound encryption mechanisms, straight-through-processing ability, teleworking has globally emerged as a main measure to contain the pandemic for many businesses. Several treasuries already adapted to teleworking conditions, while others are yet to reduce their reliance on manual procedures that require physical presence. Once business processes are adapted accordingly and a sound regulatory framework is developed, teleworking arrangements can be embedded in business continuity plans and reduce traditional reliance on secondary sites.

As reliance on ICT infrastructure increases, business continuity plans should account for cyber threats more carefully than ever. Potential threats should be analyzed in detail in terms of their likelihoods and impacts. Mitigation measures should first concentrate on prevention of risks by adhering to sound standards and practices in setting up and using ICT systems.

Country experiences on business continuity planning reveal several key lessons and principles for developing and maintaining a BCP:

- Reliance on excessive documentation is costly and may not always prove effective, especially when BCP is seen as the task of a small group within the treasury or the ICT unit. This note proposes some templates for BCP documentation.
- A short reference document, such as a pocket card, with references to more detailed resources are more useful for staff.
- With scarce resources, business impact analysis, a key component of the BCP process, can be significantly simplified for purposes of cash and debt management, focusing on time criticality of key business processes.
- Not all cash and debt management processes have to continue as normal under all conditions. Even when some business disruptions scenarios are likely to occur, if a process is not time-critical,

it can be delayed (especially when investment or measures required to reduce impact is more costly than the impact itself).

- Attention should not only focus on drafting an initial BCP, but also keeping it as a live document, with regular updates and testing.
- Maintaining the BCP should be seen as the responsibility of all treasury staff.
- Testing helps identify deficiencies in measures as well as additional risks. It also creates awareness and confidence within the treasury.

ANNEX I. BCP TEMPLATE

The following template is provided as a guide to develop a Business Continuity Plan. It should be customized to suit the specific needs of the Treasury. The *blue sample text* can be deleted after completing the template.

<insert name of the treasury> Business Continuity Plan

Date: dd/mm/yyyy

Distribution List

To assist in updating and revising the plan, an up-to-date list of all plan locations and persons supplied with a copy of the plan should be included.

Copy Number	Name	Location
01		
02		
03		

References and related documents:

Include all documents that have a bearing on your Business Continuity Plan.

Document Title
1)
2)
3)

SECTION 1

Executive Summary

An executive summary is the plan in miniature (usually one page or shorter). It should contain enough information for a reader to get acquainted with the plan without reading the full document.

Objectives

Objectives serve as a means of clarifying the purpose of the plan and should describe the intended result. An example of plan objectives is listed below:

The objectives of this plan are to:

- *undertake risk management assessment*
- *define and prioritize critical functions*
- *detail immediate response to a critical incident*
- *detail strategies and actions to be taken to enable treasury to continue operations*
- *review and update the plan on a regular basis*

SECTION 2

Business Impact Analysis

Business impact analysis can be conducted in a practical way as proposed in Annex II. The output of the BIA should be a table as in Annex Table 2.2. and should cover at least the following critical cash and debt management operations:

- Debt Servicing (loans, securities, guarantees, on-lending)
- Execution of Payment Requests (by public entities)
- Daily Cash Flow Planning
- Security Issuances via Auctions
- Loan Contracting

This should be complemented by a Business Process Analysis as proposed in Annex III. The output of the process analysis should be a table as in Annex Table 3.1.

SECTION 3

Risk Mitigation

Treasury will select the most cost effective and suitable risk treatment approach for each debt management function (assessed via BIA) using one or more of the options described at Step 2: Identify mitigation options of Section IV of this paper. See Table 3 for evaluation of several mitigation strategy options under different scenarios.

Name of Process	Scenario	Mitigation Strategy	Deadline for Completion (If Mitigation Strategy is not currently available)	Unit/Person Responsible
P1			mm/yyyy	
P2			mm/yyyy	
P(n)			mm/yyyy	

Treasury should adopt these approved mitigation strategies in order to manage/prevent an incident or event that would otherwise affect their essential/critical business activities, processes and systems. However, no essential/critical new business activities, processes and systems should be introduced until the mitigation strategies have been implemented and tested. The compliance manager will be responsible for maintaining and ensuring compliance with the requirements set out in the BCP.

SECTION 4

Incident Management Team

Should an incident or event occur that impacts on essential/critical treasury activities and/or necessitating relocation from the treasury office, an incident management team will be established to manage the relocation and/or recovery process.

The illustration in Annex IV highlights the individuals and teams and interrelationships between those responsible for managing a recovery following an incident or event.

This is to ensure that when an incident occurs, a well-defined incident management structure is in place to ensure:

- the efficient flow of information;
- consistent decision making; and
- effective communication of decisions.

Should an incident or event occur that requires building evacuation or denies access to the treasury building, an emergency center will be established at the evacuation assembly area or at a suitable alternate site. Some incidents or events may not affect all business units or the entire building. In this case, it may be practical to relocate affected staff to meeting rooms or other vacant space with the assistance of the support units.

Response

Following an incident or event, emergency response will comprise the following phases:

- *Evacuation and Containment:* includes the actions by emergency response personnel (such as floor representatives) to contain the incident, assure the safety of staff, prevent further damage or loss and ensure the treasury office is secure;
- *Assessment and Decision:* members of the incident management team evaluate the magnitude of the incident or event and decide upon a course of action and/or recovery; regarding how and where to recover essential/critical business functions. If the incident can be isolated and contained, actions are taken to restore treasury's operations using standard operating policies and procedures. It is important that all staff are made aware of their role during a recovery operation and that recovery information is clearly and regularly delivered to staff. This will be for staff to either return home until they hear otherwise or relocate to the alternate site(s).

The objective for the emergency response is to minimize the risk to treasury's business activities and operations in the treasury office by reducing or, if necessary, halting activities until the recovery infrastructure is established with the primary objective of re-establishing critical activities within recovery time objectives. To deal with the first shock of the incident, an initial action plan can be included in the pocket card as well (refer to Annex V).

Recovery

Recovery is the return to pre-emergency conditions. Performing critical activities as soon as possible after a critical incident is the primary focus.

This table should be completed with the intention of supporting recovery in 'worst case' scenarios. It can then be modified according to the degree of loss. The recovery process includes:

- developing strategies to recover business activities in the quickest possible time
- identifying resources required to recover treasury's operations
- documenting previously identified RTO's
- listing the person/s who have responsibility for each task and the expected completion date

An example is provided in the following table:

Recovery Plan

Name of Process	Scenario	Actions to be Taken	Recovery Time Objective	Unit/Person Responsible
<i>External Debt Servicing</i>	<i>S1.1</i>	<i>Teams affected by the incident go to the nearest alternative site and complete the process as usual</i>	X hours/days	<i>Debt Transactions Unit/ Name-Surname</i>
	<i>S1.2</i>	<i>If possible, teams affected by the incident go to the nearest alternative site and complete the process as usual</i>	X hours/days	<i>Debt Transactions Unit/ Name-Surname</i>
		<i>If not, teams go home and complete the process as in the alternative workflow (an illustrative modified flow is provided in Annex Table 3.2)</i>		
	<i>S2.1</i>		X hours/days	
	<i>S2.2</i>		X hours/days	
<i>S3.1</i>		X hours/days		
<i>Daily Cash Flow Planning</i>	<i>S2.2</i>		X hours/days	

SECTION 5

Rehearse, Maintain, and Review

It is critical that treasury rehearse the BCP to ensure that it remains relevant and useful. This may be done as part of a training exercise and is a key factor in the successful implementation of the BCP during an emergency. All new staff should receive basic training in business continuity as part of their orientation/induction program. Training and other maintenance tasks should be assigned to a specific unit/manager. Some important activities and exemplary timeframes are shown below:

Maintenance Activity	Timeframe
BCP documentation review and update	<i>Six monthly</i>
Technology recovery test	<i>Six monthly</i>
Staff familiarity training	<i>Annually</i>
Scenario (white board) testing	<i>At least six monthly</i>
Full test (simulated incident)	<i>At least annually</i>

Treasury should ensure that plan is regularly reviewed and updated to maintain accuracy and reflect any changes inside or outside the business. A set of scenarios and simulated live tests that can be used to test the BCP are provided in Annex VI.

The following points may help:

- A training schedule should be prepared for all people who may be involved in an emergency at the site.
- Pay attention to staff changes.
- It is best to use staff titles rather than individual names.
- If there is a change in organizational structure or suppliers/contractors, this must be amended in the plan.
- After an incident, it is important to review the performance of the plan, highlighting what was handled well and what could be improved upon next time.

Training Schedule

Record details of training schedule in the table below:

Training Date	Training type	Comments
<i>dd/mm/yyyy</i>	<i>Evacuation drill</i>	<i>All personnel evacuated and accounted for within acceptable timeframe</i>

Review Schedule

Record details of review schedule in the table below:

Review date	Reason for review	Changes made
<i>dd/mm/yyyy</i>	<i>New personnel in new roles</i>	<i>Plan updated to reflect changes to roles and responsibilities</i>

ANNEX II. BUSINESS IMPACT ANALYSIS METHODOLOGY

As mentioned in Section IV, a Business Impact Analysis (BIA) needs to cover at least four basic components:

- identification of possible scenarios/threats
- evaluation of impacts on processes
- estimation of likelihood of possible scenarios/threats
- assessment of time criticality of disruptions

Scenarios

Identification of numerous possible scenarios/threats could be simplified by representing all possible scenarios in terms of their impacts. Focusing on the ultimate impact and the duration of impact provides a practical way to assess threats. This note uses 3 basic time frames which can last for hours, days or weeks to analyze various scenarios. Annex Table 2.1 categorizes 12 scenarios under four main possible scenario themes according to their duration of impact. This categorization can be used as a basic template and other themes can be added should a sovereign has specific requirements. Scenario examples for each theme are provided in in Section IV, Table 1: Main Scenarios.

Annex Table 2.1. Main Scenarios Template

Scenario Theme	Scenarios Based on Duration of Impact		
	Intraday (a few hours)	Short-term (1–5 days)	Medium-term (> week)
S1 Physical Infrastructure Inaccessible	S1.1	S1.2	S1.3
S2 ICT System Failure (main system)	S2.1	S2.2	S2.3
S3 Staff Unavailability	S3.1	S3.2	S3.3
S4 Key Counterparty/Service Provider Failure	S4.1	S4.2	S4.3

Source: Authors

Likelihoods of Scenarios, Potential Impact on Processes and Time Criticality

After the identification of the possible scenarios, impacts on the processes, likelihood of possible scenarios and the time criticality factors need to be assessed in the BIA. Evaluation of impacts under all possible scenarios is a comprehensive and elaborate way for identifying the critical processes. Assessing the impact and likelihood on a 5x5 scale could provide a detailed picture, but it comes with the burden of extra workload. On the other hand, assessing the impact and likelihood on a 3x3 scale of “High-Medium-Low” could also provide a sound basis and could be upgraded to a 5x5 scale without much difficulty if needed. For countries where BCM practices are at the nascent stage, a simpler methodology would be useful in gaining top management’s support, participation of broader audience, and help addressing the resistance that would arise due to a more complex methodology. Thus, a 3x3 scale is used in this TNM.

Scaling definitions for impact, likelihood and time criticality used in this note are provided as a guidance below. It should be underlined that assuring consistency and a common understanding is vital. That is, everybody in the dedicated team should understand the same meaning in terms of impact and likelihood while working on a certain process and scenario. Thus, the core team and its supervisor have an important overarching responsibility for assuring consistency.

Impact:

- High: Risks will cause extensive damage and have a long-term effect
- Medium: Risks may cause considerable loss or damage
- Low: Risks have minimal/minor damage and have no long-term effect

Likelihood:

- High: Likely to occur often
- Medium: May occur intermittently
- Low: Not expected to occur but possible

Time Criticality of a process is assessed via Maximum Tolerable Period of Disruption under each scenario and same 3-scale approach is used to determine the time criticality score. In that regard, the first step is evaluating the MTPD of each process under normal conditions. Scaling for this evaluation could be as follows:

- MTPD < 1 day, meaning the process needs to be recovered in a few hours
- $1 \leq \text{MTPD} \leq 5$ days, meaning the process needs to be recovered in a few days
- $5 < \text{MTPD} \leq 30$ days, meaning the process needs to be recovered in a few weeks

In order to calculate the time criticality score, the analyst then needs to assess how the time criticality changes under various disruption durations (categorized as Intraday, Short-term and Medium-term in Annex Table 2.1). Accordingly, the time criticality score can be assigned as follows:

- Low if $\text{MTPD} > \text{Duration of Disruption}$
- Medium: if $\text{MTPD} = \text{Duration of Disruption}$
- High: if $\text{MTPD} < \text{Duration of Disruption}$

For example, a process for which MTPD is 1 to 5 days ($1 \leq \text{MTPD} \leq 5$) should have a “Low” time criticality score for an intraday disruption ($\text{MTPD} > \text{Duration of Disruption}$). However, its time criticality score should be escalated to “High” for a medium-term disruption ($\text{MTPD} < \text{Duration of Disruption}$). The logic is that processes which can be suspended for shorter periods without difficulty, could create adverse effects if halted for longer periods.

After determination of the impact, likelihood and time criticality factors a Combined Risk Score can be calculated to make a comprehensive evaluation about a process. Calculation and assessment criteria are as follows.

The Combined Risk Score is calculated by taking the likelihood, impact and time criticality factor into consideration simultaneously. By using the 3-scale approach described above, the analysts basically need to answer three questions for each possible scenario to fill out the Annex Table 2.2: The Combined Risk Score Calculation table:

- 1) What is the impact of the scenario on the process?
- 2) What is the likelihood of the scenario happening?
- 3) How is the time criticality of the process?

The **Combined Risk Score** is then constituted as: HiMeHi, HiMeMe, MeMeHi, etc. showing the effect of the Impact-Likelihood-Time Critically respectively. It presents the magnitude of the impact, likelihood of the scenario and the urgency of the recovery process in a compact way under each scenario.

The processes are deemed critical when the combined risk score has at least 2 High factors (i.e: HiHiLo, MeHiHi) or 1 High factor but 2 Medium factors (i.e: MeHiMe, MeMeHi). Critical processes and the relevant scenarios need to be covered in the BCP and the responses should be designed accordingly. Specifically, BCP should include rapid recovery procedures when the time criticality factor is High (indicated by the last two letters of the combined risk score). A filled example of Annex Table 2.2 is provided in Section IV, Table 2: Combined Risk Score Calculation Example.

Annex Table 2.2. Combined Risk Score Calculation

Processes		Scenarios											
		S1			S2			S3			S4		
		S1.1	S1.2	S1.3	S2.1	S2.2	S2.3	S3.1	S3.2	S3.3	S4.1	S4.2	S4.3
P1	<i>Impact of Scenario on the process</i>												
	<i>Likelihood of the Scenario</i>												
	<i>Time Criticality of the Process</i>												
	Combined Risk Score												
P2	<i>Impact of Scenario on the process</i>												
	<i>Likelihood of the Scenario</i>												
	<i>Time Criticality of the Process</i>												
	Combined Risk Score												
...	<i>Impact of Scenario on the process</i>												
	<i>Likelihood of the Scenario</i>												
	<i>Time Criticality of the Process</i>												
	Combined Risk Score												
P(n)	<i>Impact of Scenario on the process</i>												
	<i>Likelihood of the Scenario</i>												
	<i>Time Criticality of the Process</i>												
	Combined Risk Score												

Source: Authors

This note proposes the practical methodology above to simplify the process. However, treasuries might opt-in following a more detailed approach to conduct BIA. In the detailed approach, the risks can be identified as HiHi, HiMe, MeMe etc. by using the impact and likelihood factors in the risk assessment matrix (Annex Table 2.3) and processes with a risk score of 9 and 6 can be identified as critical. As noted earlier, a 5x5 scale can be used as well.

Annex Table 2.3. Risk Assessment Matrix

Impact (A)	Likelihood (B)	Risk Score (AxB)
High = 3	High = 3	HiHi = 9
High = 3 Medium = 2	Medium = 2 High = 3	HiMe = 6 MeHi = 6
Medium = 2	Medium = 2	MeMe = 4
High = 3 Low = 1	Low = 1 High = 3	HiLo = 3 LoHi = 3
Medium = 2 Low = 1	Low = 1 Medium = 2	MeLo = 2 LoMe = 2
Low = 1	Low = 1	LoLo = 1

Source: Authors.

More Granular Time Criticality Analysis

After identifying the critical processes, time criticality can be assessed in detail for each step in the process¹ and comprehensive response plans can be integrated to the BCP by assessing MTPDs and Recovery Time Objectives (RTOs) for each step of the critical processes on a high frequency basis as in Annex Table 2.4.

Annex Table 2.4. High Frequency Time Criticality Analysis

Process	Stage	Time	Activity	MTPD	RTO	Disruption likely to last for			
						(x) hours	(x to y) hours	(y to q) hours	> (q) hours
P1		T-n days	Activity-1	(x) hours	< x hours		BCP	BCP	BCP
		T hh:mm	Activity-2	(y) hours	< y hours		BCP	BCP	BCP
		T + n days	Activity-3	(Z) hours	< z hours		BCP	BCP	BCP

Source: Authors.

where $x < y < z \leq q$ and an area in green means no action is necessary

The granularity of the “Disruption likely to last for” column can be modified according to the severity of the process and the likely duration of the disruption when $MTPD < 1$ day for the whole process. Similarly, the hours can be replaced by days when $1 \leq MTPD \leq 5$ days, if desired. A simplified bond auction process is provided in Annex Table 2.5 for illustration purposes.

It should be noted that the BIA is not a stationary process and all components of the analysis might change over time. Thus, the BIA should be reviewed regularly (i.e. quarterly, yearly) and/or whenever deemed necessary in order to keep the analysis up to date and to reflect the effect of changing conditions in the working environment.

¹ In the simplified methodology, time criticality is assessed for the whole process under a certain scenario. However, a process usually has several steps in practice and thus, it is possible to improve the granularity of time criticality analysis in the detailed version.

Annex Table 2.5. High Frequency Time Criticality Analysis Example

Process	Stage	Time	Activity	MTPD	RTO	Disruption likely to last for			
						2 hours	(2 to 4) hours	(4 to 24) hours	> 24 Hours
Bond Auction	Pre-auction	T-7 days	Agree Auction Details	4 hours	2 hours			BCP	BCP
	Pre-auction	T-7 days	Prepare Documentation	4 hours	2 hours			BCP	BCP
	Pre-auction	T-7 days	Auction Announcement	3 hours	1 hour		BCP	BCP	BCP
	Auction	08:00–10:30	Receive Bids	1 hour	15 mins	BCP	BCP	BCP	BCP
	Auction	10:30–11:00	Process Bids	1 hour	30 mins	BCP	BCP	BCP	BCP
	Auction	11:00	Confirm Auction Results	1 hour	15 mins	BCP	BCP	BCP	BCP
	Auction	11:15	Publish Auction Results	2 hours	30 mins		BCP	BCP	BCP
	Post-auction	T + 1	Settle Auction	6 hours	2 hours				BCP

Source: Authors.

ANNEX III. PROCESS ANALYSIS TEMPLATE/EXAMPLE

Annex Table 3.1. Process Analysis and Workflow Under Normal Conditions

Name of the Process: External Securities Servicing Process							
Unit Responsible: Debt Transactions Unit							
Process Description: Preparation of payment orders and fulfilling all prior steps to complete payment obligations of the Treasury in full and on time							
Inputs of the Process	Output of the Process	Critical Resources		Performance Criteria	Processes Affected by	Affecting Processes	Risks of the Process
<ul style="list-style-type: none"> - Issuance info - Payment notices - Exchange rates - Interest rates 	- Payment order	Staff <ul style="list-style-type: none"> - Back office: Desk officer, supervisor - Head of DMO - Accounting unit: Desk officer, supervisor, accountant general 	<ul style="list-style-type: none"> - Delivery of payment order without any delays and mistakes 	- Debt servicing process of Central Bank	- External securities issuance process	<ul style="list-style-type: none"> - System failures - Network failures - Counterparty failures (Central Bank) - Disruptions longer than 4 hours - Staff mistakes 	
		Infrastructure <ul style="list-style-type: none"> - Office space - Computers with access to systems and common drives 					
		Systems <ul style="list-style-type: none"> - Debt Recording System - IFMIS 					
Person Responsible	Workflow			Control Criteria	Required Action/Resource		
Fiscal agent and paying agent	Send payment notice						
Back office desk officer	Treasury	Check payment notice & prepare payment advice			Info at the Debt Recording System	<ul style="list-style-type: none"> - Initial hardcopy document - Approve on Debt Recording System 	
Back office supervisor		Check payment advice			Info at the Debt Recording System	<ul style="list-style-type: none"> - Initial hardcopy document - Approve on Debt Recording System 	
Head of DMO		Approve payment advice			Crosscheck document content	<ul style="list-style-type: none"> - Sign hardcopy document - Approve on Debt Recording System which delivers it to Accounting Unit electronically 	
Back office desk officer		Send payment advice to accountant general				<ul style="list-style-type: none"> - Physical delivery of the hardcopies 	
Accounting unit desk officer		Accounting Unit	Check payment advice & prepare payment order			Budget approval, balance of the payment account	<ul style="list-style-type: none"> - Initial hardcopy document - Approve on IFMIS
Accounting unit supervisor	Check payment order			Budget approval, balance of the payment account	<ul style="list-style-type: none"> - Initial hardcopy document - Approve on IFMIS 		
Accountant general	Authorize payment order			Crosscheck document content	<ul style="list-style-type: none"> - Sign hardcopy document - Approve on IFMIS which delivers it to Central Bank electronically 		
Accounting unit desk officer	Send payment order to Central Bank			Crosscheck document content	<ul style="list-style-type: none"> - Physical delivery of the hardcopies 		
Central Bank back office officer	Central Bank		Setup payment in SWIFT			Crosscheck with Central Bank Registry	<ul style="list-style-type: none"> - Central Bank Information System
Central Bank back office supervisor		Check payment in SWIFT			Crosscheck with Central Bank Registry	<ul style="list-style-type: none"> - Central Bank Information System 	
Central Bank head of back office		Authorize payment in SWIFT				<ul style="list-style-type: none"> - SWIFT Software 	
Central Bank back office officer		Send payment information to DMO			Check balance of the payment account	<ul style="list-style-type: none"> - Physical delivery of the hardcopies 	
Accounting unit desk officer		Payment confirmation					

Source: Authors.

The template provided allows the user to assess:

- relevant inputs/outputs of the process
- critical resources in order to fulfill the process
- criteria to evaluate the performance of the process
- processes affecting and affected by the process
- risks associated with the process

All these elements help identify the vulnerabilities and areas for improvement in the process.

Clarifying the person in charge for each step, drawing down the process map, establishing the control criteria and identifying the necessary actions/resources, provides a solid understanding about the process. The proposed template, when complemented with the methodology used in Annex II meets the BIA requirements of the ISO 22301:2019 standards.²

In the analysis, even though there might be steps out of the treasury’s control (depending on the specific structure of the sovereign), the whole process needs to be considered in order to identify all the relevant risks and mitigation strategies. For instance, in this generic example where treasury uses the central bank as a fiscal and paying agent, the ultimate responsibility for payment rests within the treasury and there would be reputational and financial impacts if the central bank did not make the payment by the due date, albeit the payment order was sent on time and in full. This issue is identified in the “Risks of the Process” and needs to be handled as a “Key Counterparty / Service Provider Failure” scenario as discussed in Section IV (see Table 1).

Taking the recent developments in ICT, increased digitization/digitalization and precedents set by COVID-19 into consideration, the process flows need to be modified to better suit changing conditions. The process could be shortened and optimized in the BCP, instead of following the same workflow which depends on the same critical resources but only in an alternative operations site. In that regard, a modified version of the Annex Table 3.1 which depends less on physical infrastructure is provided below. In Annex Table 3.2 several steps of the process are dropped/unified and critical resources are reduced accordingly. Should the necessary regulations/authorizations for such a flowchart be put in place in advance, the process can be flexible to handle distressed conditions.

² Specifically, refer to clause “8.2.2 Business Impact Analysis” of the ISO 22301:2019 standards. This should not be mixed with compliance with the standards. Compliance of a claiming entity can only be assessed by the relevant ISO accredited institutions after inspection.

Annex Table 3.2. Process Analysis and Modified Workflow Under BCP

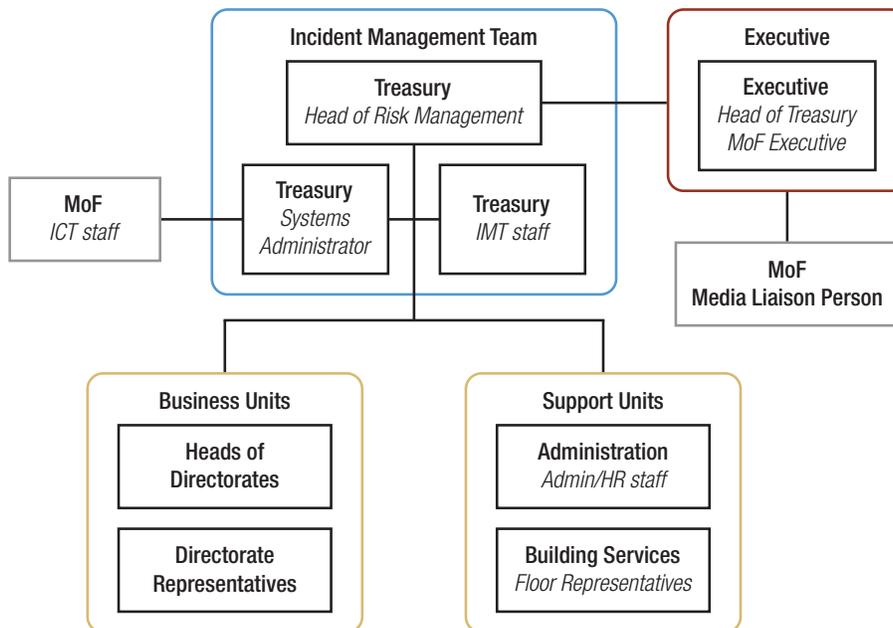
Name of the Process: External Securities Servicing Process							
Unit Responsible: Debt Transactions Unit							
Process Description: Preparation of payment orders and fulfilling all prior steps to complete payment obligations of the Treasury in full and on time							
Inputs of the Process	Output of the Process	Critical Resources		Performance Criteria	Processes Affected by	Affecting Processes	Risks of the Process
- Issuance info - Payment notices - Exchange rates - Interest rates	- Payment order	Staff - Back office: Desk Officer, Supervisor - Head of DMO - Accounting Unit: Desk officer, supervisor, accountant general	- Delivery of payment order without any delays and mistakes	- Debt servicing process of Central Bank	- External securities issuance process	- System failures - Network failures - Counterparty failures (Central Bank) - Disruptions longer than 4 hours - Staff mistakes	
		Infrastructure - Computers with access to systems and common drives (VPN)					
		Systems - Debt Recording System - IFMIS					
Person Responsible	Workflow			Control Criteria	Required Action/Resource		
Fiscal agent and paying agent	Send payment notice						
Back office desk officer	Treasury	Check payment notice & prepare payment advice		Info at the Debt Recording System	- Approve on Debt Recording System		
Head of DMO		Check/approve payment advice		Crosscheck document content	- Approve on Debt Recording System which delivers it to Accounting Unit electronically		
Accounting unit desk officer	Accounting Unit	Check payment advice & prepare payment order		Budget approval, balance of the payment account	- Approve on IFMIS		
Accountant general		Check/authorize Payment Order		Crosscheck document content	- Approve on IFMIS which delivers it to Central Bank electronically		
Central Bank back office officer	Central Bank	Setup payment in SWIFT		Crosscheck with Central Bank Registry	- Central Bank Information System		
Central Bank head of back office		Check/authorize payment in SWIFT			- SWIFT Software		
Central Bank back office officer		Send payment information to DMO		Check balance of the payment account	- Electronic delivery of the payment confirmation to Accounting Unit		
Accounting unit desk officer	Payment confirmation						

Source: Authors.

ANNEX IV. INCIDENT MANAGEMENT TEAM

The following sets out a structure for the Incident Management Team. The IMT is best headed by the person in the treasury who is head of risk management (often head of the middle office) with a team from risk management to support the head. The IMT will liaise with the business units (either with the heads of the directorates or representatives that are deemed critical to the operations of the treasury. The IMT will also liaise with the executive comprising the heads of the treasury and the MoF when necessary approvals or authorizations are needed. Support units and resources normally located in the MoF but could be within the treasury can be called upon to provide ICT resources, assist with personnel issues, and media liaison if required.

Annex Figure 4.1. Incident Management Team

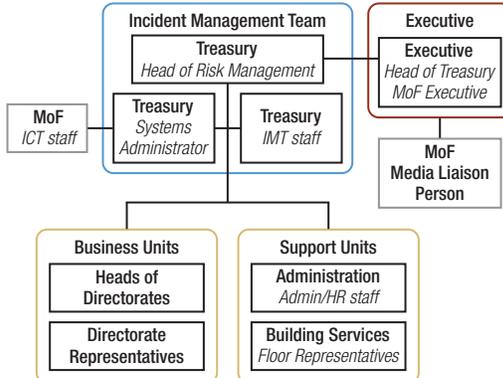


Source: Authors.

ANNEX V. POCKET CARD³

<p align="center"><Treasury Name> Incident Response Plan THIS DOCUMENT IS PRIVATE & CONFIDENTIAL Staff must keep this document with them at all times</p>	<p align="center">AFTER HOURS EMERGENCIES</p> <ul style="list-style-type: none"> • If you are on the premises after hours and an evacuation is ordered, ensure that the Director or delegate is informed. • If you are denied access to the premises when you arrive at work, go to the evacuation assembly area and await further instructions. • If you hear of an incident affecting the premises, remain at home. Make contact with Director or delegate if possible. Prepare for possible relocation to another site. 	<p align="center">OTHER EMERGENCY CONTACTS</p> <table border="0"> <tr> <td>Service</td> <td>Contact Number</td> </tr> <tr> <td>Medical</td> <td></td> </tr> <tr> <td>Security</td> <td></td> </tr> <tr> <td>Water & Sewerage</td> <td></td> </tr> <tr> <td>Gas</td> <td></td> </tr> <tr> <td>Electricity</td> <td></td> </tr> <tr> <td>Internet Provider</td> <td></td> </tr> <tr> <td>Telecom Provider</td> <td></td> </tr> </table>	Service	Contact Number	Medical		Security		Water & Sewerage		Gas		Electricity		Internet Provider		Telecom Provider		<p align="center">EMERGENCY KIT</p> <p>Documents:</p> <ul style="list-style-type: none"> • Business Continuity Plan • List of employees with contact details: home and mobile numbers, e-mail addresses, next-of-kin contact details • Procedure manuals • Lists of customer and supplier details • Contact details for emergency services • Contact details for utility companies • Contact details for local authorities <p>• Building site plan (this could help in a salvage effort), including location of gas, electricity and water shut off points</p> <ul style="list-style-type: none"> • Evacuation plan • Latest stock and equipment inventory • Bank account details <p>Equipment:</p> <ul style="list-style-type: none"> • Computer back-up tapes/disks/USB memory sticks or flash drives • Spare keys/security codes • Message pads and flip chart • Marker pens (for temporary signs) • General stationery (pens, paper, etc) • Mobile telephone with credit available, plus charger <p>Notes:</p> <ul style="list-style-type: none"> • Make sure this pack is stored safely and securely on-site and off-site (in another location) • Ensure items in the pack are checked regularly, kept up-to-date, and in good working order <p>This list is not exhaustive, and treasury should customize it to suit their organization. When it was last checked</p>		
	Service	Contact Number																			
Medical																					
Security																					
Water & Sewerage																					
Gas																					
Electricity																					
Internet Provider																					
Telecom Provider																					
<p align="center">FIRE ALARM</p> <ul style="list-style-type: none"> • Conclude phone calls immediately. • Take with you only essential portable items that may facilitate off-site recovery that are not a hindrance to evacuation. • Escort visitors to exit. • Ensure doors are closed behind you. • Evacuate the premises using nearest exit. • Assemble outside premises. • DO NOT disperse – await instructions. 	<p align="center">IF YOU DISCOVER AN INCIDENT...</p> <ul style="list-style-type: none"> • Fire: Alert other staff and call the Fire Service. • Suspicious package: Follow instructions inside back cover of emergency procedures. Alert Police. • Bomb threat: Follow instructions inside back cover of emergency procedures. Alert Police. • Stranger on the premises: Ask them who they are and who they are there to see. If they cannot provide an explanation, alert Police. • Flooding: Alert Director. Move papers, disconnecting nearby electrical equipment only if safe to do so. 	<p align="center">KEY TREASURY STAFF DETAILS</p> <table border="0"> <tr> <td>Name</td> <td>Email</td> <td>Phone #</td> </tr> <tr> <td> </td> <td> </td> <td> </td> </tr> </table>	Name	Email	Phone #				<p align="center">EMERGENCY EGRESS</p> <p align="center"><insert diagram></p>												
Name	Email	Phone #																			
<p align="center">EARTHQUAKE</p> <p>Working Hours:</p> <ul style="list-style-type: none"> • Take shelter under or next to solid furniture; move away from windows and glass partitioning. • Evacuate as above, unless it is safer staying in the premises. <p>After Hours:</p> <ul style="list-style-type: none"> • Follow all Civil Defense directives and ensure the safety of your home and family. 	<p align="center">ESSENTIAL NUMBERS</p> <table border="0"> <tr> <td>Service</td> <td>Contact Number</td> </tr> <tr> <td>Emergency Services:</td> <td></td> </tr> <tr> <td>• Fire</td> <td></td> </tr> <tr> <td>• Ambulance</td> <td></td> </tr> <tr> <td>• Police</td> <td></td> </tr> <tr> <td>Civil Defense</td> <td></td> </tr> <tr> <td>• Emergency Management Office</td> <td></td> </tr> <tr> <td>Police (Non-Emergencies)</td> <td></td> </tr> <tr> <td>• Police Station</td> <td></td> </tr> </table>	Service	Contact Number	Emergency Services:		• Fire		• Ambulance		• Police		Civil Defense		• Emergency Management Office		Police (Non-Emergencies)		• Police Station		<p align="center">FIRST AID AND CIVIL DEFENSE</p> <p>A first aid kit and civil defense resources are contained in <location> The following staff members are fully trained:</p>	
Service	Contact Number																				
Emergency Services:																					
• Fire																					
• Ambulance																					
• Police																					
Civil Defense																					
• Emergency Management Office																					
Police (Non-Emergencies)																					
• Police Station																					
<p align="center">EVACUATING THE PREMISES</p> <p>If there is damage to the building or if it must be evacuated and operations need to be moved to an alternative location, the emergency kit can be picked-up and quickly and easily carried off-site or alternatively stored safely and securely off-site.</p>	<p align="center">EVACUATION ASSEMBLY AREA</p> <p>In an evacuation, please assemble outside: DO NOT disperse until instructed to do so</p>																				

³ The pocket card has been designed to fit conveniently on both sides of an A4 page so that it can be printed and folded to credit card size, thereby fitting into a wallet, purse or credit card holder. Side 1 should show information that is for all treasury staff. Side 2 provides scope to show information that is specific to the business unit, such as contact details and checklist.

INITIAL ACTION PLAN	BUSINESS UNIT CONTACT LIST	<NAME BUSINESS UNIT> KEY ROLES AND RESPONSIBILITIES																					
<p>Management:</p> <ol style="list-style-type: none"> Key Treasury staff from risk management will form the Incident Management Team (IMT) (at the Evacuation Assembly Area, at the Recovery Site or via online meeting platform if treasury premises cannot be accessed) IMT will decide on the appropriate actions and responses after liaison with Executive Management and business units IMT will assemble the recovery teams IMT will inform rest of the staff about the situation <p>Emergency Response:</p> <ol style="list-style-type: none"> Key staff will await instructions from the IMT (depending on the timing of the event at the office, at the evacuation assembly area or at home) Key staff will invoke the recovery site Key staff will reach the Emergency Kit and activate procedures in the Response Plan 	<p>Name Organization Phone #</p>	<table border="1"> <thead> <tr> <th data-bbox="831 319 954 352">Role</th> <th data-bbox="954 319 1149 352">Designated Employees</th> <th data-bbox="1149 319 1334 352">Alternate</th> </tr> </thead> <tbody> <tr> <td data-bbox="831 352 954 428"><i>IMT Leader</i></td> <td data-bbox="954 352 1149 428">Name: <name> Contact Information: 0400 000 000</td> <td data-bbox="1149 352 1334 428">Name: <name> Contact Information: 0400 001 000</td> </tr> <tr> <td colspan="3" data-bbox="831 428 1334 596"> <p>Responsibilities:</p> <ul style="list-style-type: none"> Ensure the Business Continuity Plan has been activated Oversee smooth implementation of the response and recovery section of the plan Determine the need for and activate the use of an alternate operation site and other continuity tasks Communicate with key stakeholders as needed </td> </tr> <tr> <td data-bbox="831 596 954 672"><i>Systems Administrator</i></td> <td data-bbox="954 596 1149 672">Name: <name> Contact Information: 0400 002 000</td> <td data-bbox="1149 596 1334 672">Name: <name> Contact Information: 0400 003 000</td> </tr> <tr> <td colspan="3" data-bbox="831 672 1334 865"> <p>Responsibilities:</p> <ul style="list-style-type: none"> Ensure the Business Continuity Plan relating to ICT has been activated Oversee smooth implementation of the response and recovery of all critical systems Determine the need for and activate the use of alternate system access Communicate with treasury business units on system recovery and availability </td> </tr> <tr> <td data-bbox="831 865 954 940"><i>Compliance Officer</i></td> <td data-bbox="954 865 1149 940">Name: <name> Contact Information: 0400 004 000</td> <td data-bbox="1149 865 1334 940">Name: <name> Contact Information: 0400 005 000</td> </tr> <tr> <td colspan="3" data-bbox="831 940 1334 1142"> <p>Responsibilities:</p> <ul style="list-style-type: none"> Ensure the Business Continuity Plan that has been activated meets all statutory regulations Ensure that all treasury business units are aware and comply with all statutory regulations Determine the need for and arrange for delegated authorities needed for devolution of functions Liaise with key stakeholders where needed </td> </tr> </tbody> </table>	Role	Designated Employees	Alternate	<i>IMT Leader</i>	Name: <name> Contact Information: 0400 000 000	Name: <name> Contact Information: 0400 001 000	<p>Responsibilities:</p> <ul style="list-style-type: none"> Ensure the Business Continuity Plan has been activated Oversee smooth implementation of the response and recovery section of the plan Determine the need for and activate the use of an alternate operation site and other continuity tasks Communicate with key stakeholders as needed 			<i>Systems Administrator</i>	Name: <name> Contact Information: 0400 002 000	Name: <name> Contact Information: 0400 003 000	<p>Responsibilities:</p> <ul style="list-style-type: none"> Ensure the Business Continuity Plan relating to ICT has been activated Oversee smooth implementation of the response and recovery of all critical systems Determine the need for and activate the use of alternate system access Communicate with treasury business units on system recovery and availability 			<i>Compliance Officer</i>	Name: <name> Contact Information: 0400 004 000	Name: <name> Contact Information: 0400 005 000	<p>Responsibilities:</p> <ul style="list-style-type: none"> Ensure the Business Continuity Plan that has been activated meets all statutory regulations Ensure that all treasury business units are aware and comply with all statutory regulations Determine the need for and arrange for delegated authorities needed for devolution of functions Liaise with key stakeholders where needed 		
Role	Designated Employees	Alternate																					
<i>IMT Leader</i>	Name: <name> Contact Information: 0400 000 000	Name: <name> Contact Information: 0400 001 000																					
<p>Responsibilities:</p> <ul style="list-style-type: none"> Ensure the Business Continuity Plan has been activated Oversee smooth implementation of the response and recovery section of the plan Determine the need for and activate the use of an alternate operation site and other continuity tasks Communicate with key stakeholders as needed 																							
<i>Systems Administrator</i>	Name: <name> Contact Information: 0400 002 000	Name: <name> Contact Information: 0400 003 000																					
<p>Responsibilities:</p> <ul style="list-style-type: none"> Ensure the Business Continuity Plan relating to ICT has been activated Oversee smooth implementation of the response and recovery of all critical systems Determine the need for and activate the use of alternate system access Communicate with treasury business units on system recovery and availability 																							
<i>Compliance Officer</i>	Name: <name> Contact Information: 0400 004 000	Name: <name> Contact Information: 0400 005 000																					
<p>Responsibilities:</p> <ul style="list-style-type: none"> Ensure the Business Continuity Plan that has been activated meets all statutory regulations Ensure that all treasury business units are aware and comply with all statutory regulations Determine the need for and arrange for delegated authorities needed for devolution of functions Liaise with key stakeholders where needed 																							
RECOVERY SITE	BUSINESS UNIT CHECKLIST																						
<p>Address:</p> <p>Tel:</p> <p>Fax:</p> <p>e-mail:</p> <p>Invocation Procedure: Only key staff with the access code/key can invoke the recovery site</p>																							
OTHER IMPORTANT LOCATIONS		<p>INCIDENT MANAGEMENT TEAM</p> 																					
<p>Accounting Unit:</p> <p>Alternate Data Site:</p> <p>Building Services:</p> <p>Central Bank:</p> <p>ICT:</p> <p>....</p>																							

Source: Authors.

ANNEX VI. SCENARIO AND SIMULATED LIVE TESTS

The following provide a set of scenarios and simulated live tests that can be used to test the BCP. For the live test, the objective is to conduct these in a real-time situation whenever possible. However, the treasury will need to ensure that these tests are not conducted when very significant or critical activities are underway unless safeguards are in place to prevent any failure. The simulated live tests should be designed so as to evolve as information is made available in the order chronicled in the explanation below.

Scenario 1: System Failure

There is a system crash at 4:00pm with all treasury servers affected. The initial IT assessment is that it will take the rest of the day and all night at least to replace the servers and reinstall the operating systems, applications and data from the most recent back-up source. The Head and Deputy Head of IT and Head of the Risk Management Unit are out of the building at the time of the incident.

Scenario 2: Building Evacuation

At 11:00 am, the municipal authorities require a complete evacuation of the treasury building due to the potential risk of an explosion. Several blocks around the building are cordoned off and staff are evacuated immediately outside this zone. The authorities are not clear how long this incident will last but expect it may take more than one day to safeguard the area and allow staff back into the building. The incident occurs on the day of a government securities auction.

Scenario 3: Damage to Premises

There is a fire in the building overnight and serious damage has been incurred including significant smoke and water damage to treasury's premises. Fire authorities will not allow any access to the building due to structural damage and the risk to everyone that would enter the building. Staff arriving at the cordoned area at 7:30 am are the first to become aware of the damage.

Scenario 4: Local Pandemic

There is a pandemic (similar to the H1N1 virus of 2009). Some staff opt to stay at home to avoid contracting the virus. Staff that do come to the office are constantly monitored and as soon as they show signs of contracting the virus are immediately sent home. By the end of the week, at least 50% of staff are affected or have opted to stay at home. Staff will be required to stay at home for at least 14 days from when they were diagnosed with the virus.

Scenario 5: COVID-19 Pandemic

Several staff in treasury have tested positive for COVID-19 following a meeting where all staff were present. The health authorities immediately require the staff that have tested positive to be relocated to a quarantine facility set up by the government. Staff that have not tested positive are required to isolate at home or at the isolation facility set up by the government. Staff will be required to stay in isolation for 2 weeks. They are tested every 3 days and any that return a positive test are transferred to the quarantine area. The result is that no staff in the treasury are able to return to work in the office for 2 weeks. Staff will have internet and phone connectivity at the quarantine facility. The health authorities require treasury's premises to be thoroughly sanitized and cleaned.

Simulated Live Test #1

The substation providing power to the central city has an explosion at 9:45 am this morning with power outage across the whole of the central city. An immediate assessment by the electricity authority is that the damage is extensive, and it could take at least 1 week to repair and restore electricity completely.

Due to budget constraints in treasury and recent usage of the emergency generator, the supply of diesel is very low and expected that it may only last 3-4 hours. Due to the power outage, there is huge demand for diesel, so it may take several days before supply can be delivered.

Treasury management has decided that the generator will only be used to provide power to the two computer server rooms while the diesel lasts. This will enable IT to run critical systems and prepare to relocate to the data center.

The power outage has also affected the inner-city mobile telephone transmitting towers, so mobile phone coverage is limited in the city area. Usage of mobile phones where available has to be kept to a minimum, for example text rather than voice.

Businesses in the city area are affected and restaurants and food outlets will need to close due to lack of electricity for refrigeration.

Treasury has called an emergency meeting to activate the BCP.

Simulated Live Test #2

There is a serious explosion on treasury's premises around 5 .30pm on a working day. Around 50% of the staff are in the office at the time. 25% of the staff have left for the day and are on their way home. The remaining 25% of staff are either out of the office on business or on leave.

Treasury's premises are filled with dense smoke. Windows have been blown out and paper records and equipment are strewn across the floor. Half of the staff present at the time of the explosion have been injured, some critically, and others possibly killed. The building alarms have been activated and sprinklers are operating.

The entire building is evacuating at this point. The evacuation assembly area is rapidly congesting with evacuees and onlookers. Treasury staff that are physically able need to make a decision as to whether to evacuate or stay and administer assistance to the injured until emergency services arrive.

At 5:50 pm the fire service and ambulances have arrived, contained fires and have cleared the building of all injured staff. The impact on treasury's premises is significant. Several staff members have been confirmed dead. All uninjured staff members have congregated and been accounted for at the assembly area.

Emergency services seal the building pending investigation and cordon off the surrounding area to clear debris. All staff members are asked to go home and await further instruction. All injured staff have been treated or admitted to hospital. Staff members who had left the office have heard TV/ radio reports and notification via social media with some returning to the area to gain information or assist their colleagues.

The IMT is convened at the evacuation assembly area to activate the disaster recovery plan of the BCP. By 8:00 am the following morning the Incident Management Team has been advised that the explosion was caused by a bomb. The police and media are actively seeking information concerning the incident. An investigation is pending, and the premises have been cordoned off for at least 72 hours. The IMT has initiated the relocation strategy in consultation with the Executive team. Treasury staff are then notified of developments and given instructions on what will be their respective function.

REFERENCES

- Adelmann F., Elliot J., Ergen I., Gaidosch T., Jenkinson N., Khiaonarong T., Morozova A., Schwarz N., Wilson C., 2020, Cyber Risk and Financial Stability: It's a Small World After All. IMF Discussion Note SDN/20/07, Washington, DC. <https://www.imf.org/en/Publications/Staff-Discussion-Notes/Issues/2020/12/04/Cyber-Risk-and-Financial-Stability-Its-a-Small-World-After-All-48622>.
- Adelmann F., Gaidosch T., 2020, Cybersecurity of Remote Work During the Pandemic, IMF Monetary and Capital Market, Special Series on COVID-19. International Monetary Fund. Washington, DC. <https://www.imf.org/~media/Files/Publications/covid19-special-notes/en-special-series-on-covid-19-cybersecurity-of-remote-work-during-pandemic.ashx>.
- Allison C., 2019, Anatomy of a Bank Heist – What Exactly Happened when \$81 million Disappeared from a Bangladeshi Bank, and What Does it Mean for SWIFT? March 1, 2019, accessed on November 11, 2020. <https://fin.plaid.com/articles/anatomy-of-a-bank-heist>.
- Australian Government Department of Health, 2019, Australian Health Management Plan for Pandemic Influenza. [https://www1.health.gov.au/internet/main/publishing.nsf/Content/519F9392797E2DDCCA257D47001B9948/\\$File/w-AHMPPI-2019.PDF](https://www1.health.gov.au/internet/main/publishing.nsf/Content/519F9392797E2DDCCA257D47001B9948/$File/w-AHMPPI-2019.PDF).
- Australia National Audit Office (ANAO), 2014, Australia National Audit Office Report No.6 2014-15 Performance Audit, Business Continuity Management. https://www.anao.gov.au/sites/default/files/ANAO_Report_2014-2015_06.pdf.
- Australian Office of Financial Management (AOFM), 2016. Australian Office of Financial Management Annual Report 2015-16. October. Canberra. <https://www.aofm.gov.au/sites/default/files/2019-05/aofm-annual-report-2015-16.pdf>.
- Bank for International Settlements (BIS), 2021a, Basel Committee on Banking Supervision, Principles for Operational Resilience. March 2021. Basel. <https://www.bis.org/bcbs/publ/d516.pdf>.
- Bank for International Settlements (BIS), 2021b, Basel Committee on Banking Supervision, Revisions to the Principles for the Sound Management of Operational Risk. March 2021. Basel. <https://www.bis.org/bcbs/publ/d515.pdf>.
- Bank for International Settlements (BIS), 2021c, BIS Bulletin no:37. COVID-19 and Cyber Risk in the Financial Sector. 14 January 2021. <https://www.bis.org/publ/bisbull37.pdf>.
- Bank Negara Malaysia (BNM), 2018, Bank Negara Malaysia Press Release 29 Mar 2018. Kuala Lumpur. <https://www.bnm.gov.my/-/cybersecurity-incident-involving-the-use-of-falsified-swift-messages>.
- Brondolo, J, Aslett, J, and Komoso, A., 2020, Tax Administration: Designing a Business Continuity Plan for an Epidemic, IMF Technical Notes and Manuals TNM 2020001, International Monetary Fund, Washington DC. <https://www.imf.org/en/Publications/TNM/Issues/2020/11/10/Tax-Administration-Designing-a-Business-Continuity-Plan-for-an-Epidemic-49838>.
- Business Continuity Management (BCM) Institute, 2020, BCM Institute Glossary, accessed on: November 15, 2020. [https://www.bcmpedia.org/wiki/Maximum_Tolerable_Period_of_Disruption_\(MTPD\)](https://www.bcmpedia.org/wiki/Maximum_Tolerable_Period_of_Disruption_(MTPD)).

- Check Point Research. 2020. Cyber Attack Trends: 2020 Mid-Year Report. July 2020. <https://research.checkpoint.com/2020/cyber-attack-trends-2020-mid-year-report/>.
- Federal Emergency Management Agency (FEMA), 2018, Federal Emergency Management Agency National Continuity Programs, Continuity Guidance Circular 2018. Hyattsville. <https://www.fema.gov/sites/default/files/2020-10/continuity-guidance-circular-2018.pdf>.
- Federal Emergency Management Agency (FEMA), 2019a, Business Process Analysis and Business Impact Analysis User Guide. July 2019. https://www.fema.gov/sites/default/files/2020-07/fema_BPA-BIA-Users-Guide_070119.pdf.
- Federal Emergency Management Agency (FEMA), 2019b, Federal Emergency Management Agency National Continuity Programs, Devolution Plan/Annex Template and Instructions 2019. Hyattsville. <https://www.fema.gov/emergency-managers/national-preparedness/continuity/toolkit/brochures>.
- Financial Stability Board, 2018, Cyber Lexicon. 12 November 2018. <https://www.fsb.org/2018/11/cyber-lexicon/>.
- Government of Canada, 2013. Office of Critical Infrastructure Protection and Emergency Preparedness. A Guide to Business Continuity Planning. Ottawa. https://www.gov.mb.ca/emo/pdfs/bcont_e.pdf.
- Government of France, 2013, Secrétariat Général de la Défense et de la Sécurité Nationale. Guide Pour Réaliser un Plan de Continuité D'activité. Paris. <http://www.sgdsn.gouv.fr/uploads/2016/10/guide-pca-sgdsn-110613-normal.pdf>.
- Hämäläinen, M., Mäntylä, V., and Putkonen, P., 2018, Case Study: Bangladesh Bank Heist, ELEC-E7470—Cybersecurity Course Notes, Aalto University. <https://www.coursehero.com/file/37803306/Bangladesh-Bank-Heistpdf/>. Accessed on October 26, 2020.
- International Monetary Fund, 2017, State-Contingent Debt Instruments for Sovereigns. IMF Policy Paper. May 2017. Washington D.C. <https://www.imf.org/en/Publications/Policy-Papers/Issues/2017/05/19/pp032317state-contingent-debt-instruments-for-sovereigns>.
- International Organization for Standardization (ISO), 2019, ISO 22301:2019, ISO Security and resilience—Business continuity management systems—Requirements. <https://www.iso.org/standard/75106.html>.
- Korea Public Finance Information Service (KPFIS), 2020, Korea Public Finance Information Service, KPFIS Response to COVID 19: Learning from dBrain Operational Resiliency during Pandemic, 16 June 2020. <https://olc.worldbank.org/content/10korea-office-bbl-kpfis-response-covid-19-learning-dbrain-resilience-0>.
- Lindstedt, D. and Armour, M., 2017, Adaptive Business Continuity: A New Approach, A Rothstein Publishing Collection eBook. <https://www.rothstein.com/adaptive-business-continuity/>.
- Magnusson, T., Prasad, A., and Storkey, I., 2010, Guidance for Operational Risk Management in Government Debt Management. March. The World Bank, Washington, DC. <https://openknowledge.worldbank.org/handle/10986/27822>.

- New Zealand Government, 2015, The Guide to the National Civil Defence Emergency Management Plan. <https://www.civildefence.govt.nz/assets/guide-to-the-national-cdem-plan/Guide-to-the-National-CDEM-Plan-2015.pdf>.
- New Zealand Ministry of Health, 2017, New Zealand Influenza Pandemic Plan: A framework for action. August. Wellington. <https://www.health.govt.nz/system/files/documents/publications/influenza-pandemic-plan-framework-action-2nd-edn-aug17.pdf>.
- Nkhata S., 2017, Debt Records and Operational Risk – Support Available from International Organizations. Presentation at the 11th UNCTAD Debt Management Conference. November 13-15, 2017. Geneva. https://unctad.org/system/files/non-official-document/2017_p9_nkhata.pdf.
- Norfund. 2020. Press Release from Norfund. 13 May 2020. Oslo. <https://www.norfund.no/app/uploads/2020/05/Press-release-13052020.pdf>.
- OECD, 2020a, OECD Sovereign Borrowing Outlook. OECD Publishing. Paris. <https://www.oecd.org/finance/Sovereign-Borrowing-Outlook-in-OECD-Countries-2020.pdf>.
- OECD, 2020b, Virtual Joint Meeting of the Working Party on Debt Management and Global Forum on Public Debt Management, Agenda Item 4, Operational Risk Management and Business Continuity, 12 November 2020. Paris. <https://www.oecd.org/daf/fin/public-debt/Joint-Meeting-WPDM-Global-Forum-PDM-2020-Agenda.pdf>.
- OECD, 2021, OECD Sovereign Borrowing Outlook. OECD Publishing. Paris. <https://www.oecd.org/daf/fin/public-debt/Sovereign-Borrowing-Outlook-in-OECD-Countries-2021.pdf>.
- Pan-Canadian Public Health Network, 2018, Canadian Pandemic Influenza Preparedness: Planning Guidance for the Health Sector. Canada. <https://www.canada.ca/content/dam/phac-aspc/migration/phac-aspc/cpip-pclcp/asssets/pdf/report-rapport-02-2018-eng.pdf>.
- Proite A., Secunho L., Cabral R., 2020, Debt Management Under Extreme Circumstances: Brazil's Reactions to Covid-19 Early Events. Presentation at the World Bank Webinar. 9 April 2020. The World Bank. Washington, DC.
- Securities Industry and Financial Markets Association (SIFMA), 2020, Press Release. SIFMA Statement on Successful Completion of Industry-Wide Business Continuity Test. October 26, 2020. New York. <https://www.sifma.org/resources/news/sifma-statement-on-successful-completion-of-industry-wide-business-continuity-test/>.
- Storkey I., 2011, Operational Risk Management and Business Continuity Planning for Modern State Treasuries, IMF Technical Notes and Manuals TNM 1105, Washington, DC. <https://www.imf.org/en/Publications/TNM/Issues/2016/12/31/Operational-Risk-Management-and-Business-Continuity-Planning-for-Modern-State-Treasuries-25298>.
- The Guardian, 2016, Spelling mistake prevented hackers taking \$1bn in bank heist, March 10, 2016, accessed on: November 11, 2020. <https://www.theguardian.com/business/2016/mar/10/spelling-mistake-prevented-bank-heist>.

The World Bank, 2020, Debt Management Facility: 10-Year Retrospective 2008-2018. The World Bank. December. Washington, DC. <http://documents1.worldbank.org/curated/en/387981607701888048/pdf/Debt-Management-Facility-10-Year-Retrospective-2008-2018.pdf>.

Turkey Ministry of Treasury and Finance, 2014, Public Debt Management Report (PDMR). Republic of Turkey, July 2014, Ankara. <https://ms.hmb.gov.tr/uploads/sites/2/2018/12/Public-Debt-Management-Report-2014.pdf>.

Uganda Ministry of Finance, Planning and Economic Development. 2020. Press Release. Ministry of Finance Business Continuity Plan for COVID-19. March 27, 2020. Kampala. <https://www.finance.go.ug/sites/default/files/press/MoFPED%20-BCP%20Advisory%20%20%281%29.pdf>.

United Kingdom Department of Health, 2012, Health and Social Care Influenza Pandemic Preparedness and Response. April 2012. London. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/213696/dh_133656.pdf.