TECHNICAL NOTES AND MANUALS

Operational Risk Management and Business Continuity Planning for Modern State Treasuries

Ian Storkey

Fiscal Affairs Department

INTERNATIONAL MONETARY FUND

INTERNATIONAL MONETARY FUND

Fiscal Affairs Department

Operational Risk Management and Business Continuity Planning for Modern State Treasuries

Prepared by Ian Storkey

Authorized for distribution by Sanjeev Gupta

November 2011

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

JEL Classification Numbers:	H12, H60, H63, H83
Keywords:	business continuity, disaster recovery, business continuity and disaster recovery plan, operational risk, operational risk management, treasury operations
Author's E-Mail Address:	ian@storkeyandco.com

Operational Risk Management and Business Continuity Planning for Modern State Treasuries

Prepared by Ian Storkey

This technical note and manual (TNM)[1] addresses the following main issues:

- What is operational risk management and how this should be applied to treasury operations.
- What is business continuity and disaster recovery planning and why it is important for treasury operations.
- How to develop and implement a business continuity and disaster recovery plan using a six practical-step process and how to have it imbedded into the day-to-day operations of the treasury.
- What is needed to activate and what are the key procedures when activating the disaster recovery plan.

INTRODUCTION

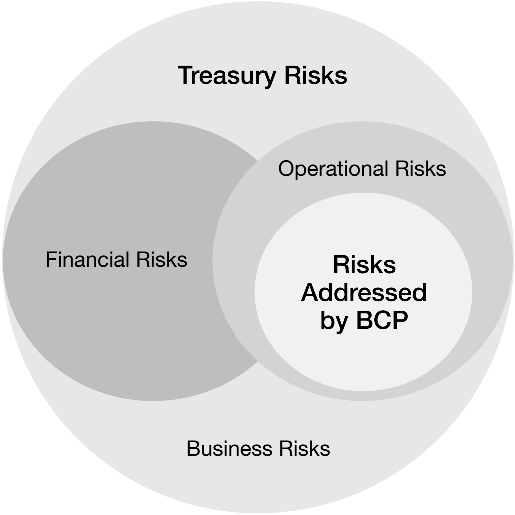
Management of financial risk is very important for the treasury operations of any ministry of finance. Ministry of finance bears responsibility for the management of very substantial government assets and liabilities, and for the management of many large value transactions, probably much more than any other government ministry or agency. The large sums involved mean that any risk exposure can have damaging financial consequences on the budget outturn and the overall government balance sheet. But there is potentially also severe reputational and political damage associated with operational errors or failures, reflecting on the competence of the ministry of finance covering treasury operations.

Ministry of finance is potentially exposed to—and will have a particular appetite for exposure to—a wide range of risks. Figure 1 illustrates the perceived risks:

- **financial risks:** traditionally managed by a risk management unit located in the ministry of finance that includes market, liquidity, and credit risks

[1] Note: Ian Storkey is an international consultant specializing in government debt and cash management and is on the Fiscal Affairs Department roster of experts. This note has benefitted from comments from Mario Pessoa (FAD), Israel Fainboim (FAD), Mike Williams (consultant) and the Mexican Federal Treasury. The author would also like to acknowledge the information obtained or provided by the governments in Australia, Chile, Turkey and United Kingdom.

Figure 1: Perceived Treasury Risks



- **business risks:** such as new legislation, change of government, macro-economic performance and any other factors affecting the ministry of finance's environment—these are often managed as part of the budget planning process
- **operational risks:** a range of threats from loss of key personnel, settlement failure, and compliance failure, to theft, systems failure and building damage—operational risk management aims to ensure the integrity and quality of the operations of ministry of finance and treasury using a variety of tools including audit, recruitment policies, system controls, and business continuity planning.

Awareness of operational risk is low in many countries, and very few ministries of finance have a business continuity and disaster recovery plan (BCP/DRP). Often it is perceived as something applicable only to the private sector and attracts little attention by senior management. This is because it is not seen as important or a priority, there are inadequate resources allocated to establish and maintain an operational risk management (ORM) framework including BCP/DRP, responsibility is delegated to information technology, and it becomes a one-off project rather than an integral part of the day-to-day treasury operations. Management neglect is often at fault with the belief that "it won't happen to me".

The problem of course is that ORM covers a wide umbrella, often seen as covering everything except for market, liquidity, and credit risks. Unlike market or credit risk, operational risk is mainly endogenous to the ministry of finance. Apart from external events such as natural catastrophes, it is linked to the business environment, nature and complexity of treasury operations, the processes and systems in place, and the quality of the management and of the information flows. There is normally no regulatory pressure to put in place adequate measures to monitor and control operational risks and maintain a BCP/DRP as is the case with central banks.

In this paper, references to the ministry of finance (MoF) should be taken to include treasury operations (managed by the treasurer), notwithstanding that some countries have a separate treasury department or agency. A debt management unit (DMU) may also be part of ministry of finance or separately constituted (e.g. as a debt management office, DMO). The DMU or DMO may perform some of the treasury operations such as cash management, although these will often be shared with or in coordination with ministry of finance.

Introduction to Operational Risk Management

Definition

Under Basel II developed by the Bank for International Settlements (BIS) [2], operational risk is defined as "the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events." The definition explicitly includes legal risk, but excludes strategic and reputation risk. While this definition and sound practices established by the Basel Committee on Banking Supervision and COSO, and usefully elaborated by entities such as TransConstellation, have been primarily designed for the banking and financial sector, the governing principles can appropriately be applied to treasury operations.[3] What is necessary is an ORM framework that is appropriate to the range and nature of treasury operations and the operating environment.

For treasury, the categories of risks, such as market risk (exchange rate and interest rate risk), liquidity risk, and credit risk are relatively well known; however operational risk is not. Government treasurers are now beginning to understand operational risk management and the importance to their treasury. A summary of operational risks faced by the treasury is set out in Box 1. Business continuity planning should be an integral part of the ORM framework for treasury.

What is ORM?

The treasurer should be aware of the major aspects of operational risks as a distinct risk category that should be managed, and should approve and periodically review the operational risk management framework applicable to treasury. The framework should provide a definition of operational risk and lay down the principles of how operational risks are to be identified, assessed, monitored, and controlled or mitigated. A risk committee may be in place to oversee this. process.

[2] Basel II "International Convergence of Capital Measurement and Capital Standards: A Revised Framework", published by the Bank for International Settlements in June 2004.

[3] The Basel Committee on Banking Supervision has members from 28 countries that provide a BIS forum for regular cooperation on banking supervisory matters. The Committee of Sponsoring Organizations of the Treadway Commission (COSO) is a joint initiative of five private sector organizations and is dedicated to the development of frameworks and guidance on enterprise risk management, internal control and fraud deterrence. TransConstellation is a Belgian not-for-profit entity in the field of financial-transaction processing with members that include Banksys, Euroclear, Fin-Force, SWIFT and The Bank of New York (Brussels office).

Box 1: Typical Treasury Operational Risks

- Infrastructure and technology failures covering computer systems, power, telecommunications, data and physical records
- Incidents where access to premises is denied, either through inaccessibility or building damage
- Dependencies on third party key service providers such as the central and/or commercial banks, telecom and internet providers, and other outsourced operations, or resource failures from such incidents as a pandemic.
- Human errors or failures through lack of resources, skills, training, policies, procedures, delegations, code of conduct, and poor management
- Failure to meet statutory, legal or contractual, human resources and other obligations including management objectives and reporting obligations
- Natural and regional disasters covering incidents such as earthquake, tsunami, severe flooding, hurricane/typhoon, volcanic eruption, severe fires, landslides and civil disturbance or terrorism

Senior management in treasury should have responsibility for implementing the ORM framework. The framework should be consistently implemented throughout all treasury operations, and all levels of staff should understand their responsibilities with respect to ORM. Senior management should also have responsibility for developing policies, processes and procedures for managing operational risk across all treasury activities, processes and systems. Senior management should also ensure that before new activities, processes, and systems are introduced or undertaken, the operational risks inherent in them is subject to adequate assessment and managed appropriately.

Treasury should implement a process to regularly monitor incidents that may cause a business disruption and/or have a serious impact on treasury operations. There should be regular reporting of pertinent information to the treasurer and senior executives in the ministry of finance. Treasury should have policies, processes, and procedures to control and/or mitigate the potentially more serious operational risks. Treasury should periodically review the ORM framework and should adjust their risk limitation and control strategies in the context of the government's overall risk management strategy and objectives. Treasury should have in place a business continuity and disaster recovery plan to ensure its ability to operate on an ongoing basis and limit losses in the event of any business disruption.

Once an ORM framework is firmly established, treasury should consider using internal and/or external auditors to independently examine and assess the framework. Ideally, the auditors should from time to time independently conduct, directly or indirectly, an evaluation of treasury policies, procedures and practices related to operational risks.

Application of ORM to Treasury Operations

As noted in the introduction, operational risk is a wide umbrella, often seen as covering everything except for market, liquidity, and credit risks. Developing an ORM framework can be an evolutionary process as it will take time and effort to not only identify and understand the risks but also the mitigation techniques in an environment that is constantly changing. There is no need to try to do everything perfectly from the outset. The framework can be developed and applied incrementally as techniques improve and staffs in treasury increasingly get to understand the risks and mitigation techniques. For the framework to succeed, it is extremely important to develop a culture of risk awareness across treasury and ensure that all staff is involved in developing and implementing the framework.

The first stage involves senior management understanding and signaling to all staff the importance attached to ORM and the need for their participation and ongoing cooperation. The principles as outlined above that will be followed in the management of operational risk need to be made clear to all staff and embedded into day-to-day operations of treasury. Each line manager needs to be made responsible for ORM in their own business area.

It is advisable that a "risk champion" be appointed to take overall responsibility for ORM. The risk champion will lead and guide the process across treasury, coordinate reporting to the treasurer and senior management, and develop the appropriate ORM policies and procedures and control environment. Ideally, the risk champion would have relevant background or experience, although this will often not be possible. There are, however, opportunities for professional training in ORM and business continuity planning which could be considered.

Once the structure has been established, the development and maintenance of an ORM framework for treasury should follow a six-step process:[4]

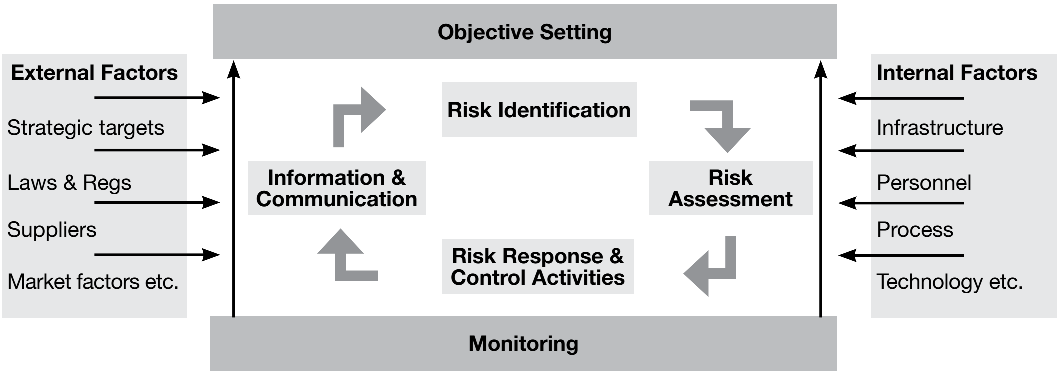
- understand and document business activities
- identify, assess and measure risks
- develop risk management strategies
- implement risk management policies, limits and controls
- monitor performance and compliance with policies, limits and controls
- process for continuous improvement of the ORM framework.

Examples of the ORM process from the Ministry of Finance in Turkey and Chile are set out in Figure 2[5] and Box 2, respectively.

[4] For more information on each of the steps, refer to "Guidance for Operational Risk Management in Government Debt Management" published by the World Bank in March 2010.

[5] Refer Hakan Tokaç and Mike Williams (2011 forthcoming).

Figure 2: ORM Model for Turkey



For treasury operations, service providers such as the central bank and commercial banks should demonstrate that they have adequate controls and safeguards when they host or process data related to banking systems. Treasury should discuss with the central bank and the commercial banks this requirement and suggest that they could use the International Standard on Assurance Engagements (ISAE) No.3402, Assurance Reports on Controls at a Service Organization, as it is a widely recognized auditing standard developed by the International Auditing and Assurance Standards Board (IAASB).[6] A service auditor's examination performed in accordance with ISAE 3402 is widely recognized, because it represents that a service organization has been through an in-depth audit of its control objectives and control activities, which often include controls over information technology and related processes. ISAE 3402 is the authoritative guidance that would allow the central and commercial banks to disclose their control activities and processes to treasury in a uniform reporting format.

The management of operational risk must be a responsibility shared and understood by all staff in treasury operations. Staff should be aware of the operational risk exposures in their area, and how they might affect business continuity, and have responsibility for managing those exposures within their own control. Senior managers should be responsible for identifying and monitoring the risks in their own units and for ensuring that the control activities work as intended and in line with priorities set by the treasurer. International experience has shown that for this all to work, ORM is more effective if a "risk champion" is appointed who is located in a risk management unit along with other risk management functions.

The risk management unit including risk champion has two roles. First, it drives the development of the risk management process, monitors performance and execution, and reports to the treasurer. Second, it acts as advisers to senior managers in identifying risks and planning

[6] On June 15, 2011, ISAE No.3402 replaced the Statement on Auditing Standards (SAS) No.70, Service Organizations that had been developed by the American Institute of Certified Public Accountants (AICPA).

Box 2: Case of Chile: Outline of the Risk Management Process

The main objective is "to have an efficient internal control system and to comply with a Risk Management process structured, consistent and coordinated for effective and efficient achievement of institutional goals and objectives".

Risk Management has the following objectives:

- Identify risks and opportunities
- Analyze the risks in the process
- Assessing risks
- Set the risk treatment
- Monitor and review (feedback)
- Construction of the risk matrix

Step 1: Risk Policy

- Define roles and responsibilities of the process of risk management
- Determine the key processes involved in improving the quality of service
- Be communicated, published and consistent with the Quality of Service Policy

Step 2: Survey Process

- Raise the processes developed by the Quality of Service Policy
- Identify risks by type

Step 3: Development of the Matrix

- Classification of transverse processes
- Process and sub-process weights
- Risk type
- Justification of strategic weighting

Step 4: Establish Ranking

- Ranking by the process set
- Establish ranking by sub-process

Step 5: Establish Treatment Plan

- Measures, timelines, responsibilities, potential impact (reduce, accept, avoid, sharing) and performance indicators, measurement period goal

Step 6: Monitoring and Review

- Generating reports
- Monitoring
- Diagnosis and improvement proposals

Strategic Risk Matrix

Information Processing				Critical Risk Information				Key Control			
Process	Sub-process	Stage	Objective	Critical Risk	Probability	Impact	Severity	Control	Design	Control Effectiveness	Risk Exposure

control activities. In practice, the unit typically evolves over time, from being the main driver when first establishing the ORM framework including BCP/DRP, to being more of a facilitator or adviser when it is running smoothly.

Business Continuity and Disaster Recovery Planning

Introducing Business Continuity and Disaster Recovery Planning

Business continuity management or planning is the development, implementation and maintenance of policies, frameworks and programs to assist treasury manage a business disruption, as well as build treasury resilience. Resilience comes from tackling the likelihood as well as the consequences of disruptive events. Therefore, it is important to have both effective ORM and business continuity planning frameworks in place. Business continuity planning assists in preventing, preparing for, responding to, managing, and recovering from the impacts of an incident or disruptive event.

Business continuity means maintaining the uninterrupted availability of all key business resources required to support essential treasury operations. Treasury's business strategies and decisions are based on an assumption of the business continuing. An event that violates this assumption is a significant occurrence in the life of any treasury, impinging directly on its ability to fulfill its business objectives and the reputation of the treasury and the government. Among other things, business continuity planning is about putting in place measures that seek to prevent business interruption events from occurring in the first place. It also encompasses establishing appropriate responses should such an event occur.

Business continuity planning is therefore that part of ORM that establishes cost-effective measures should an event occur. As such, it deals with actual events—a risk event which has occurred—and the action required responding to the event. To this extent, it complements the overall ORM process which deals foremost with possibility of occurrence of risks events that may occur, and the analysis and pro-active management of such events. Treasury faces a variety of risks. These may be sourced externally, and therefore largely out of the immediate control of treasury, or internally. Internal risks arise both at the strategic (MoF-wide) level and at the operational (business process) level.

Business continuity planning should address the subset of operational risks where environmental factors or poor operational controls raise the potential for loss of or damage to treasury operations (including people, information, infrastructure, and premises). With the support of all staff, treasury should maintain a BCP/DRP that the government and external counterparties will view as sound practice, and which will play an important part in the overall approach to ORM. BCP/DRP concentrates on improving resilience and ensuring mitigation techniques are put in place for those areas identified as having a combination of very-high/high probability and catastrophic/

Figure 3: Trade-off between Cost and Recovery Time

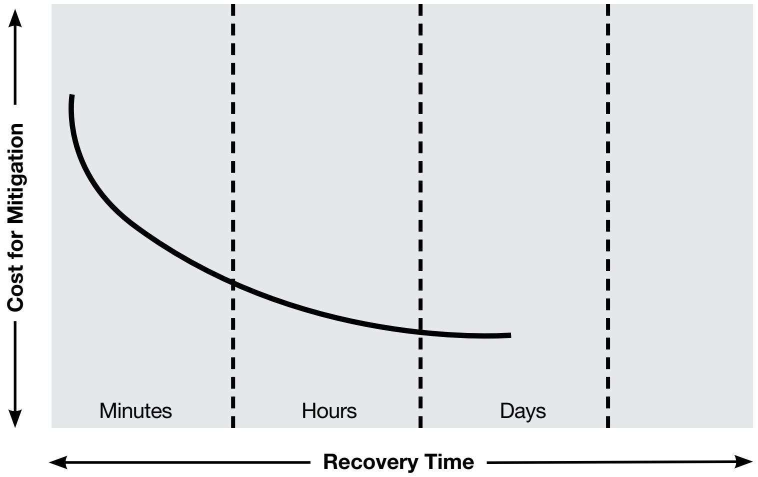


Figure 3 is drawn from page 4 of Australian National Audit Office (2009), with the modification to show non-linearity as the cost of mitigation is likely to increase exponentially if the recovery time is reduced to minutes rather than hours and days.

major. It is also advisable to cover incidents of lower probability that have a catastrophic/major impact. How these are defined is set out in the business impact analysis section below.

Treasury should select the most cost effective and suitable risk intervention approach for each activity using one or more of the following strategies:

- **prevention or avoidance**, where the probability of an event occurring is reduced or eliminated by, for example, installing back-up power generators, using more than one telecom provider, training staff, and implementing fraud prevention policies and procedures
- **transference**, where risks are passed to third parties by taking out insurance or outsourcing with BCP/DRP incorporated in service level agreements
- **containment**, where the potential impact of an event occurring is limited in the early stages using controls or other techniques by implementing fraud detection policies and procedures, putting in place escalation procedures so that treasury management can respond immediately should an event begin to escalate, and having more than one person to perform a particular task or activity
- **acceptance and recovery,** where an event or disruption might well occur but treasury operations can be resumed successfully using the disaster recovery plan that is regularly tested at the recovery location (alternate site)

While some strategies 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 treasury. Therefore, a key element for treasury to consider is the cost-recovery time trade-off as can be seen from Figure 3. The cost-recovery time trade-off will not be linear as the cost to shorten the recovery time, particularly if it is necessary to recover critical activities, processes, and systems, within minutes will require significant investment in replication of systems, mirroring of data, redundancy of communication and infrastructure, and an alternate site that is quickly activated.

The cost of establishing and maintaining an alternate site could be high, not only in terms of the initial investment in the facility and all the equipment needed but also in terms of maintaining each system and renewing the equipment when changes or updates are made at the primary site. Also, it is important to ensure that the alternate site is sufficiently far away from the primary site so that both are unlikely to be affected by the same incident or event. For example, it would be important to ensure that the alternate site is located on a different power grid and/or provider as well as a different telephone exchange and/or provider so that both sites are not impacted simultaneously. Regularly using the alternate site for training and testing can provide some benefits to compensate for the cost.

The recovery of treasury's most critical activities, processes and systems are likely to be hours or for some activities 1-2 days, although there could be end-of-day activities or processes that may need to be completed before day's-end. In these cases, it may be more cost effective to prepare manual processes which can be activated if a disruption occurs. The cost-recovery trade-off should be considered as part of the business impact analysis and the mitigation strategies that treasury will implement.

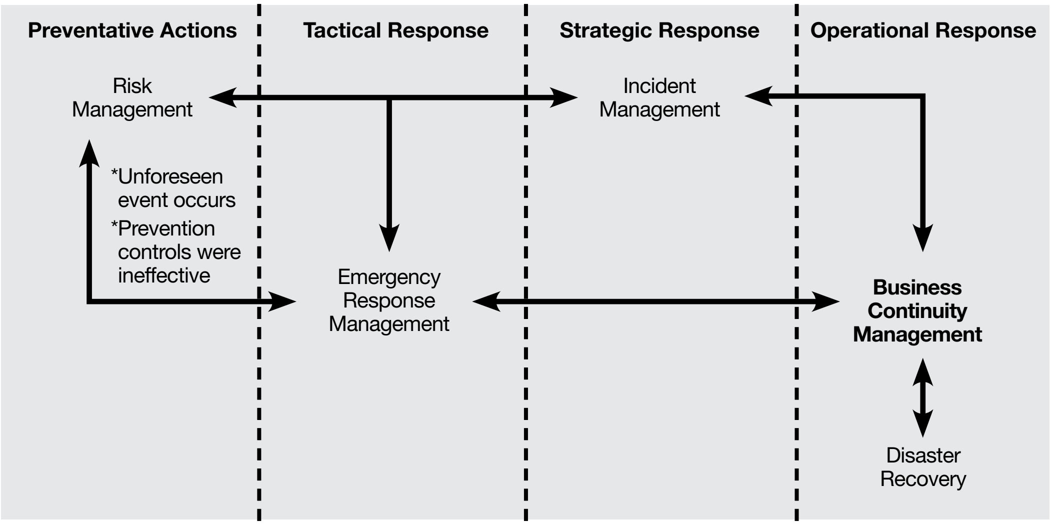
Importance of BCP/DRP to Treasury Operations

The relationship between operational risk, emergency response, incident and business continuity management or planning for a business disruption or event is shown in Figure 4. These management activities are scalable, depending on the operating context of the treasury. It may be that in a small, non-complex or less time-critical treasury, some or all of these activities are combined. In a treasury that is large, complex, or geographically dispersed, the use of separate emergency response, incident management and business continuity management teams increases the need for clear roles and responsibilities, and effective communication. The focus of this TNM is business continuity management or planning.

Treasury's policy for business continuity planning should be to:

- perform a business impact analysis, and develop mitigation strategies, which will ensure the continuity of its business, operations and technology components in the event the existing environment is unavailable;
- develop and maintain a comprehensive business continuity and disaster recovery plan (BCP/DRP) to ensure that essential/critical treasury activities are recoverable;
- business continuity planning and the BCP/DRP should be developed in accordance with international standards such as the Business Continuity Management standard BS-25999 or International Standards Organization ISO-27031; and

Figure 4: Relationships in Managing a Business Disruption



Source: Page 2 of Australian National Audit Office (2009).

- report the status of business continuity planning and the BCP/DRP annually to the treasurer and senior management in the ministry of finance.

The BCP/DRP for treasury should be an integral part of the ORM framework and developed to ensure that the following objectives are met:

- government's interests are protected in terms of reputation, reporting and resource impact, and impact on treasury operations;
- government meets all statutory, contractual and market obligations;
- should an essential/critical activity be disrupted by an incident or event, this activity is re-established within the designated recovery period using the DRP; and
- BCP/DRP is an integral part of treasury's day-to-day operations and that it is regularly updated with ongoing staff training and testing.

Six-Step Process to Develop a BCP/DRP

To develop the BCP/DRP, a six-step process is recommended as follows (each step is described in more detail in the next section):

- **Step 1:** Document business activities and critical processes and systems
- **Step 2:** Undertake business impact analysis to assess probability and impact
- **Step 3:** Develop BCP/DRP (include third parties)
- **Step 4:** Implement or update BCP/DRP
- **Step 5:** Training to imbed into the day-to-day operations of the treasury
- **Step 6:** Regular (annual) testing and updating

Developing a BCP/DRP

Step 1: Document Business Activities

The first step is for treasury to fully understand the activities, processes and systems and identify the key risks that might impact on their operations. Process maps and process-flow analysis can be used along with existing procedure manuals to understand treasury operations. The risk champion suggested above can oversee this process to ensure a common understanding and consistency of approach and terminology. This should be at a level that will balance the amount of detail and usefulness to senior management and the overall process.

The key is to identify critical processes and systems and the time period when these processes and systems are required. This will determine the criticality of each activity, process and system in terms of the time period (minutes, hours or days) that treasury is unable to maintain essential/critical operations. A table of essential/critical systems should be developed and maintained by treasury (an example is provided as Table 1 below). It will set out the time period when each system is required, the data that will be recovered from the back-up, and the location where the system can be accessed should an incident occur.

TABLE 1. TREASURY CRITICAL SYSTEMS FRAMEWORK

System	Time Period (minutes, hours or days)	Data Back-up (time and location)	Access Location (alternate site or data center)

Step 2: Business Impact Analysis

A business impact analysis will involve everyone responsible for treasury operations, including the more junior staff, as it helps to develop a risk understanding and a risk culture within treasury. This can be done by convening workshops and brainstorming sessions for each treasury function. For each category of operational risk and incident that may affect treasury as set out in Table 2, treasury should assess the risk exposures as a result of an incident or event affecting their operations. This requires separately assessing the probability and the impact, for example using a combination of Very-High / High / Medium / Low / Very Low Probability and Catastrophic / Major / Moderate / Minor / Insignificant Impact from a reputation, reporting and resource, or impact on treasury operations perspective as explained in Table 3.

TABLE 2. INCIDENTS THAT MAY AFFECT TREASURY OPERATIONS

Infrastructure and Technology Failures		
Power failure	Hardware failure	Software failure
Data corruption including viruses	LAN/WAN/Intranet/ Internet failure	Internal flood (sprinklers, pipes)
Voice network failure	Theft of equipment	Theft of data/information
Poor maintenance	Accidental damage	Sabotage
Incidents where Access to Premises is Denied		
Flooding or a fire concern	Health and safety violation	Hazardous chemicals accident
Gas or chemical leak	Industrial action or riot	Bomb or terrorist threat
Building fire or explosion	Internal/external flood	Sabotage or terrorism
Key Service Providers or Resource Failures Dependencies		
Failure of key service providers (telephone, internet, banking etc)	Third party providers (Central Bank and other outsourced operations)	Impact of incident on critical teams or groups (pandemic, travel, group incident)
Staff, Management and Related Human Failures		
Human error (which may be due to poor training or inadequate supervision)	Poor training or inadequate supervision (which may lead to human error or execution of unauthorized transactions)	Failure to follow code of conduct or conflict of interest guidelines
Lack of policy guidance (which may lead to poor decisions or unauthorized activities)	Poor understanding of risk environment (which may lead to unnecessary or unknown risks)	Poorly specified delegations (which may lead to execution of unauthorized transactions)
Failure to follow or adhere to administrative practices (which may lead to processing errors)	Key person risk (which may lead to human error when key person is absent)	Fraudulent, corrupt or dishonest practices (which may lead to financial loss and political embarrassment)
Failure to Meet Statutory, Legal, Human Resources and Other Obligations		
Legal/statutory obligations (e.g. compliance with loan agreements)	Management directives (e.g. internal policies and procedures)	Procedures manuals and delegated authorities
Reporting obligations (e.g. to higher authorities and international institutions)	Contractual obligations (e.g. debt service obligations)	Health and safety regulations (e.g. national workplace laws or regulations)
Major Natural and Regional Disasters		
Major earthquake	Hurricane, cyclone or tornado	Tsunami
Volcanic eruption	Severe fires	Civil disturbance
Severe flooding	Landslides	Terrorism

Not all operational risks will be of equal importance for treasury as this will be specific to the environment and risks faced. For treasury, there are three impacts that may need to be considered with the analysis:

- **Reputation**al impact: that may lead to a loss of confidence by the government, loss of market confidence, media coverage, and/or a high-level ministerial or Parliamentary enquiry

TABLE 3. MEXICO IMPACT CRITERIA FRAMEWORK			
Assessment of Impact	**Reputational Impact**	**Reporting & Resource Impact**	**Impact on Treasury Operations**
Catastrophic	Loss of Government confidence Loss of market confidence Loss of trust, e.g. States & Ministries Extensive media coverage High-level ministerial enquiry [or resignation] Financial and legal penalties	Reported to President or Congress Significant amount of time spent dealing with impact (i.e. greater than 20 person-days)	Failure to pay high priority payments on due date (personnel, debt service, tax refunds, States, taxes) To incur an erroneous payment such as crediting funds in the wrong account or deliver after the due date To incur payment default penalty (as no budgetary resource) such as, debt service, tax refunds, payroll and transfers to entities (with political impact) Incur an overdraft in bank account Unable to transfer between treasury´s accounts due to the failure of the central bank´s payment systems and of commercial banks Unable to receive or access revenues Unable to transact in foreign currencies (receive, buy, sell or invest) Unable to access treasury's bank accounts or its balances and operations
Major	Strained Government relationships Temporary loss of market confidence Moderate media coverage Ministerial enquiry Strained relationships with taxpayers and the discouragement of them to pay taxes	Reported to Minister Large amount of time spent dealing with impact (i.e. between 10 and 20 person-days)	Failure to pay government contractors and/or subsidies, which would bring financial and political consequences because of payment delays Delay to pay the holder of a deposit or application for funds Unable to identify the concept of revenue Unable to issue reports for the operation and registration of revenues, and for official forms Unable to issue the certificate of received payment to the taxpayer Unable to open the vault that protects the official forms Inconsistent reports of bank accounts and their transactions and balances

TABLE 3. MEXICO IMPACT CRITERIA FRAMEWORK

Assessment of Impact	Reputational Impact	Reporting & Resource Impact	Impact on Treasury Operations
Moderate	Increased Mexican Government attention Market confidence not affected Minor, if any, media attention Major attention within MoF Holder's deposit and taxpayers confidence is moderately affected	Reported to the entity responsible for monitoring treasury Moderate amount of time spent dealing with impact (i.e. between 5 and 10 person-days)	Failure to transfer funds to other Government agencies for minor expenses (revolving funds), and obligations that could be paid the following working day
Minor	Some Government attention No media coverage Internal MoF enquiry Taxpayers' attention	Included in internal treasury reports Some amount of time spent dealing with impact (i.e. less than 5 person-days)	Same day delay in sending the payment layout to the central bank An official requirement to central bank for extending banking hours Unable to place investments Unable to deliver timely reports to the accounting office Partial delivery of official forms and bills Unable to access the database of the authorized officers to instruct disbursements, as well as of the authorized signatures for withdrawals of deposits from third parties
Insignificant	Government and market relationships intact No media coverage	No reports needed Minimal amount of time spent dealing with impact (i.e. less than 5 person-hours)	Unable to operate from the main offices that causes a delay in payment executing timetable Errors in the electronic files of revenues sent to the accounting centers Same day delay in the payment to deposit holders Moderate delay in the delivery of the order of official forms

The table is based on the framework developed for the Federal Treasury in Mexico. The author would like to acknowledge the effort of treasury staff that helped to prepare the impact criteria framework.

- **Reporting and resource impact:** that may be reported to the government or senior management within government–or external to regulators–and/or significant time is spent dealing with the issue

- **Impact on treasury operations:** that may result in failure to meet treasury's payment and other obligations and maintain the treasury activities for the effective functioning of the government

Under each of the three impacts, treasury should undertake an assessment of what are the factors that will impact according to each of the five assessment categories. An example of how this can look is shown in Table 3. Clearly, this table will vary according to the activities that are the responsibility of treasury and the priorities that are assigned or implicit in treasury operations.

For each business activity, process and system used in the business impact analysis, treasury will then associate a probability to the occurrence of an incident/event and also an impact rating assuming that the incident/event were to occur. Those activities assessed by treasury with a rank of 4 and 5 are identified in the event of an incident according to Table 4. Depending on its risk tolerance level, treasury may wish to also include the rank of 3, particularly where the impact could be catastrophic either in terms of reputation, reporting and resource, or impact on treasury operations.

The final key element of the business impact analysis is the time criticality of each system and process across treasury operations. This requires assessing the maximum period that treasury can be without access to the system or process before it materially impacts on its operations under any of the categories above. It is normal to categorize each system or process using time periods such as by end-of-day, within 24 hours (it could be less if needed), 48 hours, 72 hours, 5 business days, or more than 5 business days. Table 1 can be used for this purpose.

A detailed mitigation strategy then needs to be developed for those incidents or events that are ranked as 4 and 5 in Table 4. If the number of incidents or events with these rankings is high, the matrix will clearly signal that there is a need for an alternate site and a well documented disaster recovery plan. The BCP/DRP will then set out critical information such as (1) critical systems and processes; (2) contact lists for key staff/teams; (3) standard procedures when invoking the plans; and (4) details of the recovery infrastructure including teams and documentation to be stored in the treasury office (primary site) and recovery location (alternate site).

Step 3: Develop Business Continuity and Disaster Recovery Plan

Once the business impact analysis has been completed, treasury should develop strategies that concentrate on improving resilience and ensuring mitigation techniques are put in place for those incidents or events ranked as 4 and 5 in Table 4. For these areas, treasury should select the most cost effective and suitable risk treatment using one or more of the responses set out above. A business continuity planning report is then submitted to senior management on the greatest risks, the techniques to mitigate, control, or limit the risks, the actions that are recommended to address the greatest exposures including activation of a DRP, and an estimate of costs. Senior management can then assess the

TABLE 4. RISK/IMPACT MATRIX

		Impact Level of Risk				
		Insignificant	Minor	Moderate	Major	Catastrophic
Likelihood Level of Risk	Very High	3	4	4	5	5
	High	2	3	4	4	5
	Medium	2	2	3	4	4
	Low	1	2	2	3	4
	Very Low	1	1	2	2	3

cost-risk trade-off before making decisions and seeking approval from the treasurer and/or senior management in the ministry of finance.

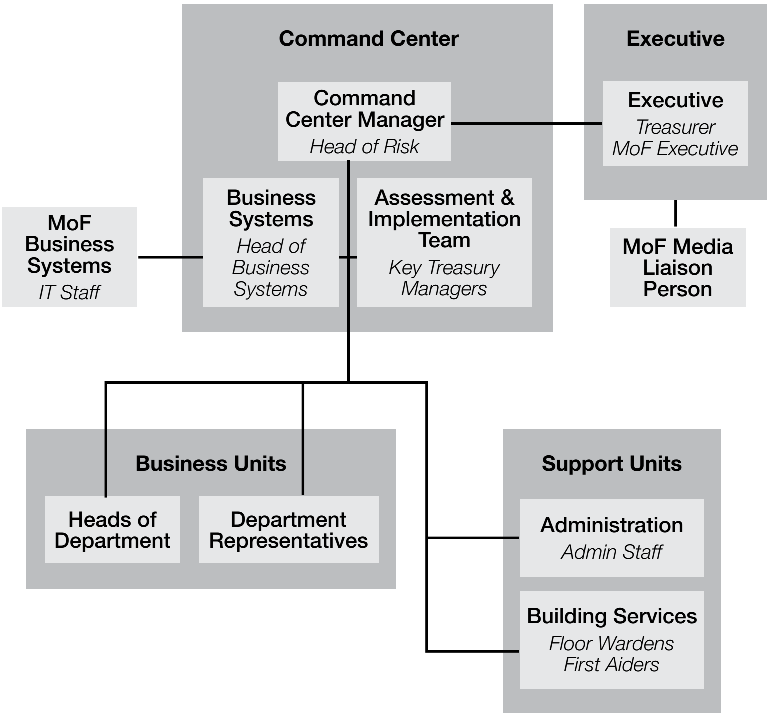
An integral part of business continuity planning will be a Disaster Recovery Plan (DRP) which documents the recovery component of the BCP. It facilitates the (i) smooth transition to recovery operations following a major incident or event (or disaster); (ii) escalation of recovery operations in the event of a prolonged disruption; and (iii) return to normal operations as quickly as possible. An important part of the DRP is the structure of incident management and recovery teams along with the administration and IT support. An example of a command center structure is provided as Figure 5.

Step 4: Implement the BCP/DRP

Once the BCP/DRP has been approved, the risk champion or risk management unit can oversee the implementation of the BCP/DRP and incorporate it into the wider ORM monitoring and control policies and procedures for treasury. This will include raising awareness with external parties to cover all activities external to treasury of the BCP/DRP and ORM framework in order that they understand their respective roles in maintaining business continuity and during the activation when required of the DRP. The risk champion or risk management unit will be responsible for maintaining and ensuring compliance with the requirements set out in the BCP/DRP.

Treasury should also introduce the requirement that third party providers have in place a BCP/DRP and this should be included in service level agreements or a memorandum of understanding. These third parties would include the central bank, providers of telecommunication and banking services, and relevant external IT providers. It would also be useful for treasury to integrate its BCP/DRP with other critical systems such as the government's integrated

Figure 5: DRP Command Center Structure



financial management information system (IFMIS), debt recording and management system, and other key systems in ministry of finance.

Step 5: Training

Staff in treasury needs to understand its roles and responsibilities in compliance with the BCP/DRP and wider ORM policies and procedures. They may also need to take on additional responsibilities to introduce and maintain risk-reduction or mitigation strategies for their respective area. The BCP/DRP should include a section on training with training exercise/scenarios and the frequency of such training.

Training should be managed by the risk champion or risk management unit and undertaken for all treasury staff members and should consist of:

- awareness presentations for existing employees (may also possibly be incorporated into a treasury orientation/induction program for new employees)
- provision of a training manual
- interactive training (Intranet)

If treasury has an alternate site, this can provide a valuable training facility as regular testing at the alternate site can be integrated with the training program. For example, it will enable staff in treasury to become familiar with the alternate site and how treasury opera-

TABLE 5. DRP TIMEFRAME FOR MAINTENANCE AND TESTING

Maintenance	Timeframe
BCP/DRP documentation review and update	six monthly
Technology recovery testing	six monthly
Staff familiarity testing	annually
Scenario (white board) testing	annually
Full test (simulated incident)	annually

tions can be run should an incident or event occur that may lead to relocation. While it is normal to rely on experienced staff that are deemed critical to treasury operations, this process can broaden knowledge and experience in order to reduce key person risk. Moreover, critical staff may not be available when an incident or event occurs and other staff can be called upon to provide the necessary backup in this situation. Some organizations have staff permanently at the alternate site with staff that can be rotated. This both ensures familiarity, and facilitates a quick start-up. It also allows continuity in the event that the primary site is completely destroyed.

Step 6: Regular Testing and Updating

No matter how well designed and thought-out the BCP/DRP may seem, international experience shows that it will very rarely work in practice without realistic and robust testing. The critical systems and processes of treasury should be tested annually and the BCP/DRP updated based on the results of each test and the need for continual improvement. It is important each system and process be individually tested. Testing can be disruptive as it requires commitment of staff to ensure sufficient resources are available. It is not recommended the BCP/DRP be tested as a whole as this would be resource intensive and may affect normal operations–unless it is at the weekend. A test exercise using a scenario approach is one option (this can involve a walk-through test or activation of DRP and testing at the alternate site) but a 'live' test is viewed as the only way to fully test the DRP. The testing could be done in conjunction with the testing of the other systems such as IFMIS and the central bank's own DRP. An example of the maintenance and testing of the BCP/DRP is shown in Table 5.

Maintaining the BCP/DRP requires an ongoing monitoring process to assess its effectiveness and whether it is in accordance with the wider ORM policies and procedures. This is achieved through a combination of ongoing monitoring activities and periodic testing including the annual testing of the DRP. Ongoing monitoring occurs in the normal course of treasury operations; and it is the responsibility in the first instance of line managers, with coordinating responsibility assigned to risk champion or risk management unit. As was noted earlier, the BCP/DRP can be improved over time as experience develops, particularly when there is a history of incidents or events and their impact in terms of reputation, reporting and resource, or impact on treasury operations. The six-step process set out above should be revisited on an annual basis, although the first step may just involve an update of the business activities, processes and systems reflecting changes from the previous assessment.

All new business activities should be reported to the risk champion or risk management unit during the planning phase. As for changes to existing procedures and systems, these will also be reported to the risk champion or risk management unit. Business cases should include an evaluation of business continuity risks, and project budgets must include adequate provision for appropriate preventative and recovery countermeasures. No critical systems or new business activities should be put into production until suitable recovery arrangements have been implemented and tested.

Activating the Disaster Recovery Plan

Command Center Structure

Should an incident or event occur that impacts on essential/critical treasury activities and/or necessitate relocation from the primary site, an incident management process will be established in a command center to manage the relocation and/or recovery. Figure 5 sets out 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 or event occurs, a well-defined incident management structure is in place to ensure:

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

In the event of an incident or event, staff that has been pre-nominated and are available will relocate to the alternate site to recommence business. This simplifies the logistics of planning the recovery, reduces confusion amongst staff, and allows telephone diversion plans to be prepared and lodged with the telecom providers in advance. A degree of flexibility will be needed to cater for different incidents. However, the number of recovery locations used should be kept to a minimum to facilitate staff communication and emergency management.

Should an incident or event occur that requires building evacuation or denies access to the building, the emergency command center will need to be established in the alternate site (if this is in place) or some designated location. 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 business systems and support vendors. Increasingly, the ability to work from home has become a viable and effective option in some incidents. For example, with the H1N1 pandemic, staff in the Treasury in Mexico that were confined to their homes but well enough to work were set up to work from home. This is more feasible with web-enabled systems, good internet services, encryption, and firewalls that are put in place beforehand.

The primary role of the command center is for the coordination, control and exchange of information across treasury. The command center team initiates the decision-making process for problems and major incidents that may or may not require business relocation. Crisis management and decisions of an immediate nature are also part of the responsibility of the team. This will include managing communications with external parties, such as the media and major external groups.

Members of the command center and associated groups include:

- ministry of finance senior management and the treasurer
- representative(s) from business systems/IT
- representatives from support services such as HR, administration and/or building services

The responsibilities of all command center members will be to meet at the emergency command center location (alternate site if available or another designated location) in order to:

- provide a central point of contact for all matters relating to the recovery operation for staff, suppliers, and media
- facilitate the collection and collation of information relating to the status of the emergency and progress of the recovery
- facilitate the distribution of instructions to staff, counterparties, and other affected third parties

The responsibilities of the command center team include:

- quickly making the decision to invoke recovery activities based on available information
- coordinating communications with ministry of finance
- manage communications with the media either directly or through a media liaison person
- maintain the flow of information to staff, counterparties and other key stakeholders
- approve significant expenditure associated with the recovery
- monitor compliance requirements throughout the recovery process
- ensure that effective security is maintained in the locations where recovery activities are being undertaken
- determine how the scope of recovery activities will be escalated in the case of significant incidents
- plan and manage the restoration and recommissioning of the treasury primary site

Business systems should address the recovery of essential/critical IT infrastructure processes and systems. Some will involve the input of third parties to initiate call diversion and assist in

Box 3: Case of UK DMO – Business Recovery Management

Objectives

In addition to the Incident Management Plan, further procedures are necessary to ensure the individual business operations are recovered in an effective and timely manner. Guidance on the steps to follow is covered under Business Recovery Management.

Business Recovery Management is used in conjunction with the Impact Analysis component of the BCP. Whereas the Impact Analysis will provide a status report of how an incident may affect certain critical functions, Business Recovery Management looks at how the business operations are recovered following the incident.

The Impact Analysis provides actions and workarounds for specific critical processes. Business Recovery Management is used to assess and determine approaches to restoring key business operations.

Business Recovery Steps
Step 1: Business Assessment (Managers and/or Team Leaders)

- Establish the current status of each business activity
- Confirm IT system and resource availability for each business activity
- Assess market conditions following any widespread incident
- Establish status of key stakeholders

Step 2: Status Report (Managers and/or Team Leaders)
Provide status reports to senior management for each business area including:

- High priority activities to be completed
- Activities that will be suspended
- Systems that are currently unavailable
- Resource requirements and availability
- Feedback from stakeholders

re-routing other communications facilities. Treasury should ensure that service level agreements with key third party information providers reflect recovery requirements and include the provision for participation in testing exercises.

Business systems role will also include managing the:

- restoration of the e-mail, internet and other essential communication services
- restoration or rerouting of electronic payment or banking systems with central bank and any commercial banks
- retrieval of back-up data and restoration of data to resume critical functions at the recovery location

Step 3: Prioritization

- Management responsible for each business area to determine the order of priorities for their respective areas
- Senior Managers to confirm priorities of key business operations and communicate to Managers and Team Leaders
- IT to be made aware of system requirements based on business priorities

Step 4: Decision-making

- Any strategic decisions referred to appropriate forums.
- Decisions on whether to suspend or cancel any specific operations
- Decisions should be documented and reported to relevant business areas

Step 5: Implementation

- Individual teams to implement agreed business activities using any manual work-arounds as identified in the Impact Analysis
- Staff to report progress and completion of activities to management so that subsequent assessments and prioritizations can be made
- Any statements to stakeholders made in respect of any revised or suspended activities

Step 6: Returning to Main Office Location

Once the building manager has given clearance for reoccupation of main office location and the systems & telecommunications infrastructure have been restored, the remigration will require:

- Validation that the infrastructure has been restored through testing by business areas, coordinated by Team Leaders
- A detailed plan of migration to be prepared by the IT management team including synchronizing and testing the cutting back of systems and re-setting the disaster recovery site–the detail of this will depend on the nature and impact of the original incident
- Senior Management Group should meet and agree a communication strategy involving an announcement to the market and advising key contacts of the remigration

- procurement, configuration and deployment of additional user workstations, peripheral equipment, network and cabling capacity, phone lines and handsets
- procurement, configuration and deployment of additional server equipment and telephony services to support the escalation of recovery activities when recommissioning of the treasury primary site is likely to take more than, say, two weeks
- third party liaison to provide user support
- technology project management of the restoration and recommissioning of the treasury primary site
- cut-over to normal operations and decommissioning of temporary services

Support services (HR, administration and building services staff) will be expected to report to the command center team and provide assistance as directed. This may include:

- tracking staff whereabouts and ensuring staff safety and welfare
- answering the phones and relaying messages
- contacting staff to relay messages and confirm availability
- arranging catering, accommodation, trauma counseling, emergency payments, organisation of child care, staff rotation etc
- ensuring security is enforced at the incident and any temporary recovery location
- facilitation of insurance claims and emergency purchasing
- redirection of mail and couriers

Emergency Response

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

- **Evacuation and Containment:** includes the actions by emergency response personnel to contain the incident, assure the safety of staff, prevent further damage or loss and ensure the treasury primary site is secure
- **Damage Assessment:** members of the command center team (including business systems and support services) evaluate the magnitude of the incident or event and decide upon a course of action and/or recovery
- **Recovery Decision:** based on the damage assessment, a decision is made regarding how and where to recover essential/critical business functions. If the incident or event can be isolated and contained, actions are taken to restore treasury 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

The objective for the emergency response is to minimize the risk to treasury's business activities and operations in the primary site. This is achieved by reducing or if necessary halting activities until the recovery infrastructure is established with the primary objective of re-establishing critical activities within 24 hours (or if needed by the end-of-day) and other essential activities within 48-72 hours.

Each staff member should be issued with an information sheet and important contact details (treasury, ministry of finance and central bank), including existing mobile and home telephone numbers, external contact details, and treasury key contacts. This information can be made available in a format that can be stored on treasury staff mobile phones, iPads, laptops or other media for ease of access and recovery of this information.

Business Recovery

Once a course of recovery action has been decided upon, business recovery will follow in this order:

- **Activate Recovery Infrastructure:** the BCP for systems and communications infrastructure needs to be invoked with inbound calls being diverted and key production systems reverting to the alternate site. For all essential/critical applications, data will be accessed at the alternate site from restored systems or through a data center if applicable. For services provided by third parties such as the central bank, staff may be able to relocate to third party premises to work from designated systems.
- **Survival Level Operations:** initially the business activities at treasury or the alternate site should be limited to core activities. For less time-critical functions, these can be temporarily suspended and/or staff directed to work from home.
- **Escalation:** if the incident is severe enough to warrant an extended period away from the primary site (generally exceeding two weeks), business activity may be escalated since a prolonged period at survival level operations could exacerbate the impact of the incident, affect the ability of treasury to maintain essential/critical activities, processes, and systems, and cause undue stress for staff. Where practical, escalation priorities can be predetermined with indicative timeframes noted for the recovery of each business activity or process.
- **Primary Site Recommissioning:** this includes actions taken to salvage, restore or replace damaged or lost property, facilities and services at the primary site and the process of recommencing business at the primary site.

Post Incident Review

A comprehensive review can then be carried out to ensure that the recovery plan and infrastructure are updated or improved based on the experience of the incident. In particular, each of the six-step processes can be examined to identify weaknesses and/or omissions and the results used to revise and update the BCP/DRP. This may lead to changes to business processes, underlying infrastructure including systems and facilities at the alternate site, enhanced training, and testing among other changes identified in this phase.

Conclusion

Putting in place an ORM framework including a BCP/DRP should be seen as a priority for any treasury given the operational risks that they face and critical functions and activities that they perform. The development of a BCP/DRP should not be seen as a one-off project but should become an integral part of the day-to-day operations of treasury. The six-step process to develop, implement, test and maintain the BCP/DRP will provide the treasury with the practical steps needed to ensure that this occurs.

References

Australian National Audit Office (2009), *Business Continuity Management: Building Resilience in Public Sector Entities, Best Practice Guide–June 2009* [http://www.anao.gov.au/~/media/Uploads/documents/business_continuity_management_.pdf]

Bank for International Settlements (2003), *Sound Practices for the Management and Supervision of Operational Risk*, Basel Committee on Banking Supervision [http://www.bis.org/bcbs/index.htm]

British Standards Institution (2006), *Business Continuity Management: Code of Practice* [http://www.bsigroup.com/en/Assessment-and-certification-services/management-systems/Standards-and-Schemes/BS-25999/]

Committee of Sponsoring Organizations (COSO) of the Treadway Commission (2008), *Internal Control–Integrated Framework: Guidance on Monitoring Internal Control Systems, Volumes I, II and III* [http://www.coso.org]

Hakan Tokaç and Mike Williams (2011 forthcoming), *Government Debt Management and Operational Risk: A Risk Management Framework, and how it was applied in Turkey*, OECD/EU

International Organization for Standardization (2011), *ISO-27031: Information Technology–Security Techniques–Guidelines for Information and Communication Technology Readiness for Business Continuity* [http://www.iso.org/iso/catalogue_detail?csnumber=44374]

TransConstellation (2007), *Best Practices in Qualitative Operational Risk Management: The ORM Reference Guide* [http://www.transconstellation.com]

TransConstellation (2007), *Roadmap to Operational Risk Management Success: The ORM Maturity Benchmark* [http://www.transconstellation.com]

World Bank (2010), *Guidance for Operational Risk Management in Government Debt Management*, Tomas Magnusson, Abha Prasad and Ian Storkey [http://siteresources.worldbank.org/INTDEBTDEPT/RelatedPapers/22491571/OperationalRiskManagement201003.pdf]

Annex: BCP/DRP Checklists[7]

The following provides a set of checklists and templates that can be used to develop the BCP/DRP.

CHECKLIST 1: IMPLEMENTATION OF BCP		
Characteristics of Sound Practice BCP/DRP in Treasury Operations	**Completed Yes/No**	**Level of Implementation (Basic/Mature)**
Characteristic 1: An ORM framework including BCP/DRP is in place.		
Characteristic 2: Training and awareness of BCP/DRP has been conducted.		
Characteristic 3: A risk assessment has been conducted.		
Characteristic 4: A business impact analysis has been conducted.		
Characteristic 5: Preparatory controls have been implemented.		
Characteristic 6: Treasury has documented and senior management has endorsed BCP/DRP.		
Characteristic 7: BCP/DRP testing and exercises have been conducted.		
Characteristic 8: A risk champion or risk management unit is monitoring BCP/DRP.		

CHECKLIST 2: IDENTIFY CRITICAL BUSINESS PROCESSES AND SYSTEMS	
Identify Critical Business Processes and Systems	**Completed Yes/No**
Document and confirm Treasury’s objectives and performance criteria.	
List all critical business processes and systems which underpin achievement of objectives.	
Rank the processes and systems in order of importance to the Treas ury’s objectives and exclude those processes not considered critical to achieving the objectives.	
Review the functional organisation chart to identify general areas of operational responsibility.	
Obtain any supporting documentation that is available which would provide a summary of critical business processes and systems.	
Interview managers responsible for critical business processes and systems to confirm understanding.	
Consider process interdependencies that exist: • within Treasury and MoF • with external or third parties	

[7] The checklists have been drawn from Australian National Audit Office (2009) and modified to cover treasury operations.

CHECKLIST 2: IDENTIFY CRITICAL BUSINESS PROCESSES AND SYSTEMS

Identify Critical Business Processes and Systems	Completed Yes/No
Determine the minimum requirements necessary to perform each critical process. Consider: • activities • resources • people: ○ facilities (including building and equipment); ○ technology (including IT systems and applications); ○ telecommunications; ○ vital records; • interdependencies • other	
Obtain senior management endorsement of the prioritized list of critical business processes.	

TEMPLATE: REQUIREMENTS NECESSARY TO PERFORM EACH CRITICAL PROCESS OR SYSTEM

Critical Business Process or System #< >:	**<insert process name>**
Activities	
Resources	
People	
Facilities (including buildings and equipment)	
Technology (including IT systems and applications)	
Telecommunications	
Vital Records (including paper and electronic)	
Interdependent Processes (including internal and external)	
Other	

Note: repeat for each critical process or system.

CHECKLIST 3: UNDERTAKING A BUSINESS IMPACT ANALYSIS

Undertaking a Business Impact Analysis	**Completed Yes/No**
Gather relevant existing information such as: • disruption scenarios • emergency response management plan • incident management plan • pandemic plan • IT disaster recovery plan	
Consult key personnel and business units: • each Treasury business unit including risk management • IT including MoF IT • internal audit • building and facilities • MoF senior management • external or third parties	
Evaluate the impact of a loss of each critical process or system using the Treasury's impact analysis criteria: • reputation • reporting and resource • treasury operations	
Identify interim procedures (alternative or manual processing) techniques to be adopted during the recovery phase.	
Determine the maximum tolerable period of disruption for each critical process or system.	
Determine internal and external critical interdependencies.	
Identify vital records (paper and electronic).	
Determine the recovery time objective for each critical process and IT system or application.	
Determine s the recovery point objective for electronic data.	
Estimate the time to overcome the backlog of work accumulated during a business disruption incident or event.	
Obtain senior management endorsement of the business impact analysis.	

CHECKLIST 4: EXAMINING OPTIONS TO MINIMIZE DISRUPTIONS	
Considerations for Selecting Activities and Resource Alternatives	**Considered Yes/No**
In selecting alternative activities and/or resources, the following activities are addressed: • people • facilities (including building and equipment) • technology (including IT systems and applications) • telecommunications • vital records • interdependencies • other	
Document a brief description of each option to minimize the effects of a business disruption event.	
Determine other resources required and the cost for each option (this may require information from third parties).	
Compare recovery options, including cost, in light of recovery priorities and the maximum tolerable period of disruption.	

CHECKLIST 5: ALTERNATE SITE CONSIDERATIONS	
Considerations for Alternate Site (to be activated by the DRP)	**Considered Yes/No**
The characteristics of the alternate site indicate adequate physical security and appropriate environmental controls.	
The risk profile of the alternate site is different to that of the Treasury's primary site so that both locations are unlikely to be affected by the same disruption. For example, there is sufficient distance from the Treasury's primary site, different power grid and different telephone exchange.	
Contracts clearly specify the availability of alternate site and the rights of individual subscribers in the event of multiple disaster declarations.	
Amount and nature of support services that will be provided at the alternate site: • implementation assistance • support for testing • logistical support • after hours support	
The number of Treasury staff that is needed at the alternate site and limitations on numbers if any that are imposed by the facility.	
Limitations imposed on the use of the alternate site and whether there is scope to extend/renew contract in the event of a major and prolonged disruption and use of the alternate site.	
The amount of time and availability for testing at the alternate site.	
Treasury is able to periodically audit the installations of systems at the alternate site to ensure that the specified configuration is maintained.	

TEMPLATE: TABLE OF CONTENTS FOR BCP/DRP

Section	Information Contained
Cover Page	Title and version Concise Statement of objective of BCP/DRP Senior management endorsement
Table of Contents	Contents of BCP/DRP
Activation	Steps to be taken immediately after an incident or event occurs (emergency response) Escalation process Criteria for activation of DRP
Roles and Responsibilities	Command center structure Roles and responsibilities of all teams
DRP	Team assembly arrangements Recovery steps (procedures, task and action lists) Alternate site relocation
Resource Requirements	People Facilities (including building and equipment Technology (including IT systems/applications Telecommunications Vital records Interdependencies Other
Communication	Communication protocol Sample communications (e.g. team activation message, press release, staff broadcasts etc) Media liaison
Event Log	Event log template
Contact Lists	Emergency services contact list Internal team contact list Dependent organizations contact list External/stakeholder contact lists Staff contact lists
Other Information	Instructions, maps, diagrams and other useful information for staff

TNM/11/05

International Monetary Fund
Fiscal Affairs Department
700 19th Street NW
Washington, DC 20431
USA
Tel: 1-202-623-8554
Fax: 1-202-623-6073