IAN STORKEY
INTERNATIONAL CONSULTANT

Debt Management Office Business Continuity Plan

Istanbul, Turkey
10-12 May 2016

ADB

2016 Asian Regional Public Debt Management Forum

BCP – Why Necessary for DMOs?

There is often a clear misconception in many countries that as long as the IT Department makes a backup of the debt database on a regular basis (i.e. daily or weekly), stores the data offsite in a secure location, and has an alternate data site with backup servers, the debt management office (DMO) can be seen to have an effective business continuity and disaster recovery plan (BCP/DRP).

An IT BCP/DRP omits many elements for effective business continuity, which needs to focus on critical processes, systems, and people in the DMO

Often DMO management deny or ignore that there are critical risks to their business operations

DeMPA DPI-13 (Dimension 3) has requirement for BCP/DRP

Costs can be high, reputation is at risk, but government's finances are critical, particularly in the case of a major incident such as a regional or national disaster

Purpose of the DMO BCP

The Business Continuity Plan (BCP) establishes the operational procedures to maintain the critical functions of the DMO and the guidelines to reactivate the critical or essential procedures in one or more alternate sites

Scope of the DMO BCP

The BCP focuses on the basic elements of operational continuity of the DMO:

- **critical functions/activities, key personnel, critical systems [the key focus]**
- alternate facilities and remote operation
- order of command succession and delegation of authority tables

The BCP presents the development of procedures to guarantee operational continuity applied to all the spectrum of threats and emergencies that could affect the DMO

DMO Policy for the BCP

1. 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

2. Develop and maintain a comprehensive business continuity and disaster recovery plan (BCP/DRP) to ensure that essential/critical DMO activities are recoverable (business continuity planning and the BCP/DRP will be developed in accordance with international standards such ISO 22301)

3. Report the status of business continuity planning and the BCP/DRP annually to the Head of the Ministry of Finance

Threats to the DMO

Infrastructure and Technology Failures		
Power failure	Hardware failure	Sabotage
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	Cyber attacks
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 (travel, food poisoning, group incident)

Source: World Bank 2010

Threats to the DMO

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		
Earthquake	Hurricane or severe flooding	Tsunami
Volcanic eruption or landslide	Severe fires	Civil disturbance or terrorism

Source: World Bank 2010

Impact on the DMO

Assessment of Impact	Reputational Impact	Impact on DMO's Operations	Reporting & Resource Impact
Catastrophic	Loss of Government confidence Loss of market confidence Loss of trust, e.g. Subnationals & Line Ministries Extensive media coverage High-level ministerial enquiry [or resignation] Financial and legal penalties	Failure to pay debt service payments by the due date To incur an erroneous payment such as payment to the wrong account or payment of an incorrect amount To incur debt service payment default penalty Failure to conduct auction of government securities To execute trading or hedging transactions without authority or in excess or limits or controls Failure to meet legal or contractual obligations with international bond issues	Reported to Prime Minister or Parliament Significant amount of time spent dealing with impact (i.e. greater than 20 person-days)
Major	Strained Government relationships Temporary loss of market confidence Moderate media coverage Ministerial enquiry	Unable to transact in foreign currencies (e.g. receive, buy, sell or invest in USD) Failure to deliver reports to all stakeholders by the deadline required To submit reports to the government with significant errors and/or poor advice Significant errors in debt service forecasts with an adverse impact on the budget outcome Failure to make cheque payments Loss or damage of loan agreements and loan transaction records	Reported to Minister of Finance Large amount of time spent dealing with impact (i.e. between 10 and 20 person-days)

Impact on the DMO

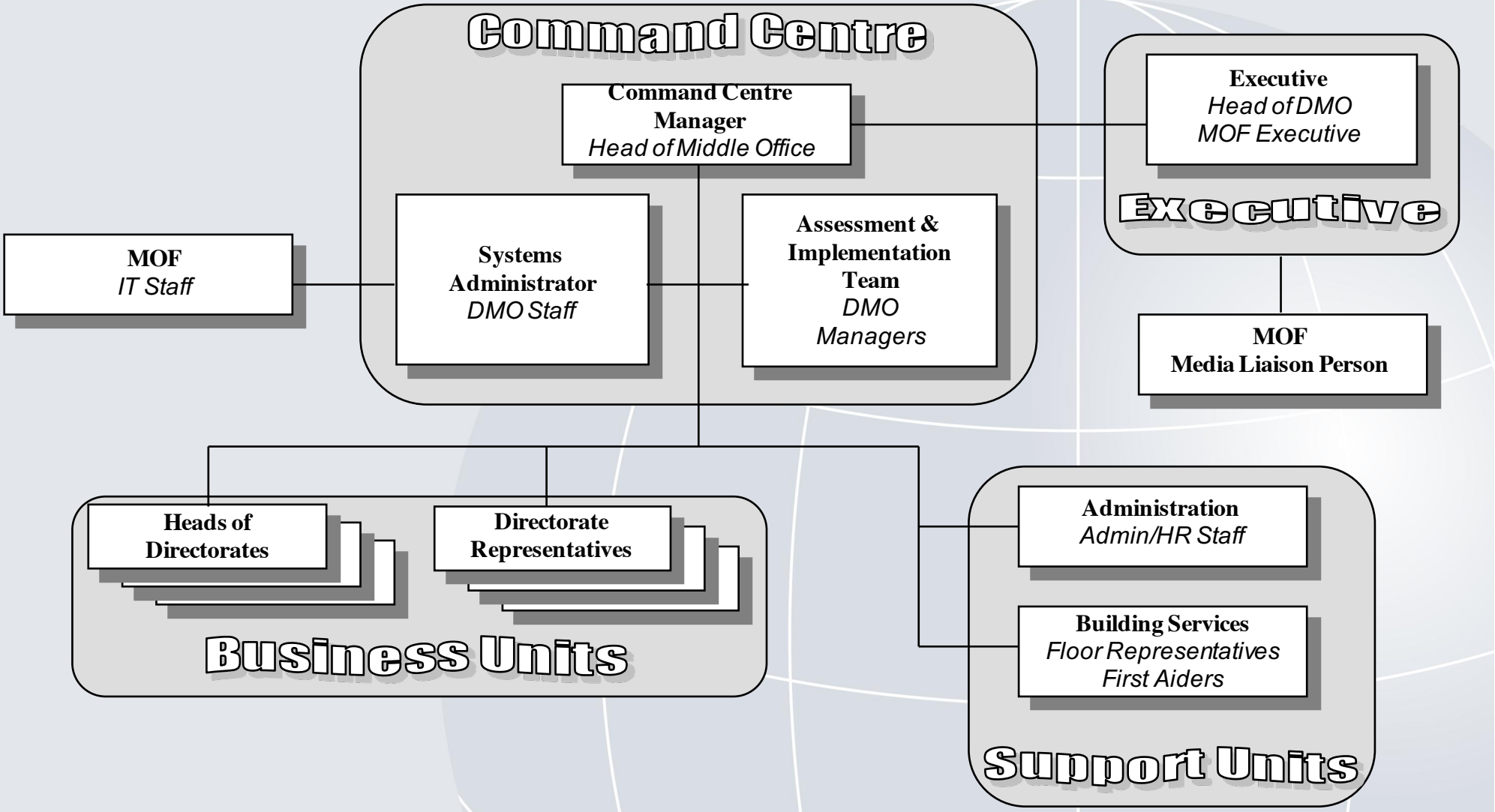
Assessment of Impact	Reputational Impact	Impact on DMO's Operations	Reporting & Resource Impact
Moderate	Increased Government attention Market confidence not affected Minor, if any, media attention Major attention within DMO	Failure to undertake critical debt management activities Incorrect recording of debt and debt transactions in the DRMS Failure to prepare debt service forecasts by the due date Failure to complete evaluations for authorization to contract new debt or for on-lending within imposed deadlines Failure to evaluate cost/pricing of contingent liabilities	Reported to the entity responsible for monitoring the DMO Moderate amount of time spent dealing with impact (i.e. between 5 and 10 person-days)
Minor	Some Government attention No media coverage Internal DMO enquiry	Failure to monitor and report on market conditions Failure to undertake analysis of the debt portfolio Errors on the DMO website Unable to conduct reconciliation of debt records with creditor statements	Included in internal DMO reports Some amount of time spent dealing with impact (i.e. less than 5 person-days)
Insignificant	Government and market relationships intact No media coverage	Errors in setting up users and permissions in the DRMS Failure to monitor audit trails in the DRMS	No reports needed Minimal amount of time spent dealing with impact (i.e. less than 5 person-hours)

Probability and Impact: Turkish Treasury

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

Source: Hakan Tokaç and Mike Williams (2013)

Incident Management



BCP Strategy

- **Prevention or avoidance**, where the probability of an event occurring is reduced or eliminated
- **Transference**, where risks are passed to third parties such as insurance or outsourcing
- **Containment**, where the potential impact of an event occurring is limited in the early stages using controls or other techniques
- **Acceptance and recovery**, where an event or disruption might well occur but debt management operations can be resumed successfully using the disaster recovery plan

Source: World Bank 2010

Templates for the DMO to Complete

System	Time Period (minutes, hours, days)	Desired Time Period (minutes, hours, days)	Location of the Server (Primary Site)	Data Back-up (time and location)	Access Location (alternate site or data centre)

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	

Process: <Insert Process Name>

Persons involved:
Critical Person 1:
Critical Person 2:
Critical Person 3:

Id	Critical Activity	System(s)	Description
1.1			
1.2			
1.3			

BCP Template for the DMO

1	**EXECUTIVE SUMMARY**
1.1	BCP Objectives
2	**INTRODUCTION**
2.1	Scope
2.2	Audience
2.3	Reference Documents
3	**BUSINESS CONTINUITY PLAN**
3.1	Approach
3.2	Categories of Operational Risks
3.3	Purpose and Policy
3.4	Risk Assessment and Business Impact Analysis
3.5	Risk Mitigation Strategies

4	**DISASTER RECOVERY PLAN**
4.1	Incident Management Structure
4.2	Command Centre
4.3	Recovery Process
4.4	Recovery Infrastructure
4.5	Recovery Process
4.6	Training and Testing
4.7	DRP Checklist
5	**MAINTAINING THE BUSINESS CONTINUITY PLAN**
5.1	Assigning Responsibility for BCP to the Compliance Manager
5.2	Integrating BCP into the day-to-day Operations of DMB
5.3	Maintenance of the BCP

Can also include Wallet/Pocket Card for each business unit

THANK YOU

Contact Details:

Ian Storkey

Email: ian@storkeyandco.com

Website: http://www.storkeyandco.com

Operational Risk Management References

- Bank for International Settlements (2003), **"Sound Practices for the Management and Supervision of Operational Risk"**, Basel Committee on Banking Supervision http://www.bis.org/publ/bcbs96.pdf

- Hakan Tokaç and Mike Williams (2013), **"Government Debt Management and Operational Risk: A Risk Management Framework, and how it was applied in Turkey"** SIGMA Paper No.50, OECD and the EU http://www.sigmaweb.org/publications/SIGMA_SP50E_2013.pdf

- International Monetary Fund (2011), **"Operational Risk Management and Business Continuity Planning for Modern State Treasuries"** Technical Note and Manual (TNM1105) by Ian Storkey http://www.imf.org/external/pubs/ft/tnm/2011/tnm1105.pdf

- World Bank (2010), **"Guidance for Operational Risk Management in Government Debt Management"** by Tomas Magnusson, Abha Prasad and Ian Storkey http://treasury.worldbank.org/bdm/pdf/Guidance_OperationalRiskManagement_Mar2010_Magnusson.pdf

Country BCP/DRP 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/uploads/documents/Business_Continuity_Management_.pdf
- Government of Canada (2012), **"A Guide to Business Continuity Planning"** http://www.dufferincounty.ca/files/content-pdf/bcp.pdf
- French General Secretary of Defense and National Security (2013), **"Guide pour Réaliser un Plan de Continuité D'Activité"** http://www.sgdsn.gouv.fr/IMG/pdf/Guide_PCA_SGDSN_110613_normal.pdf
- New Zealand Ministry of Civil Defence and Emergency Management (2015), **"The Guide to the National Civil Defence Emergency Management Plan 2015"** http://www.civildefence.govt.nz/assets/guide-to-the-national-cdem-plan/Guide-to-the-National-CDEM-Plan-2015.pdf

Other Relevant References

- 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"** Volume I and II

  http://www.coso.org/documents/volumei-executivesummary.pdf

  http://www.coso.org/documents/volumeii-guidance.pdf
- Committee of Sponsoring Organizations (COSO) of the Treadway Commission (2009), **"Internal Control – Integrated Framework: Guidance on Monitoring Internal Control Systems"** http://www.coso.org/documents/coso_guidance_on_monitoring_intro_online1_002.pdf
- International Organization for Standardization (2011), **"ISO-27031: Information Technology–Security Techniques–Guidelines for Information and Communication Technology Readiness for Business Continuity"** https://www.iso.org/obp/ui/#iso:std:iso-iec:27031:ed-1:v1:en