IAN STORKEY
INTERNATIONAL CONSULTANT

Debt Management Office
Business Continuity Plan

World Bank WebEx Meeting

January 27, 2016

Sri Lanka 2004

Chile 2010

Japan 2011

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.

And often DMO management deny or ignore that there are critical risks to their business operations.

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

BCP – Why Not Addressed by DMOs?

- **Mainly executive neglect:**
  - "it won't happen to us" is alive and well
  - inadequate resource allocation
  - low priority
  - responsibility delegated
  - project versus program
  - relative lack of regulatory pressure
- **How well prepared is the DMO?**
  - does the DMO have a BCP/DRP?
  - is business continuity viewed within an ORM framework?
  - has the BCP/DRP been tested in the last 12 months?
  - is the BCP/DRP managed by IT or middle office?

Central Banks are normally better prepared than the DMO, as they often have a BCP/DRP including the recovery infrastructure such as an alternate site and regularly test

Debt Management Performance Assessment (DeMPA) Requirements

- **DPI 12:** Debt Administration and Data Security
- **Dimension 4:** Frequency and off-site, secure storage of debt recording and management system backups

- **DPI 13:** Segregation of Duties, Staff Capacity, and Business Continuity
- **Dimension 3:** Presence of an operational risk management plan, including business continuity and disaster recovery arrangements

Assessment for DPI 12 (Dimension 4)

Score C	• Debt recording and management system backups are made at least once per month • Backups are stored in a separate, secure location where they are protected from incidents such as theft, fire, flood, or other incidents that may damage or destroy any of these backups
Score B	• ***Plus…*** debt recording and management system backups are made at least once per week and are stored in a separate, secure location
Score A	• ***Plus…*** debt recording and management system backups are made daily and stored in a secure filing system before they are moved to the separate, secure location weekly

Assessment for DPI 13 (Dimension 3)

Score C	• There is a written business continuity plan and DRP, which has been tested in the past three years
Score B	• ***Plus…*** documented guidelines exist for operational risk management
Score A	• ***Plus…*** there is an operational recovery site that is tested at least annually

Purpose of the DMO BCP

- The BCP, or Business Continuity Plan presents a planning and action plan, 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

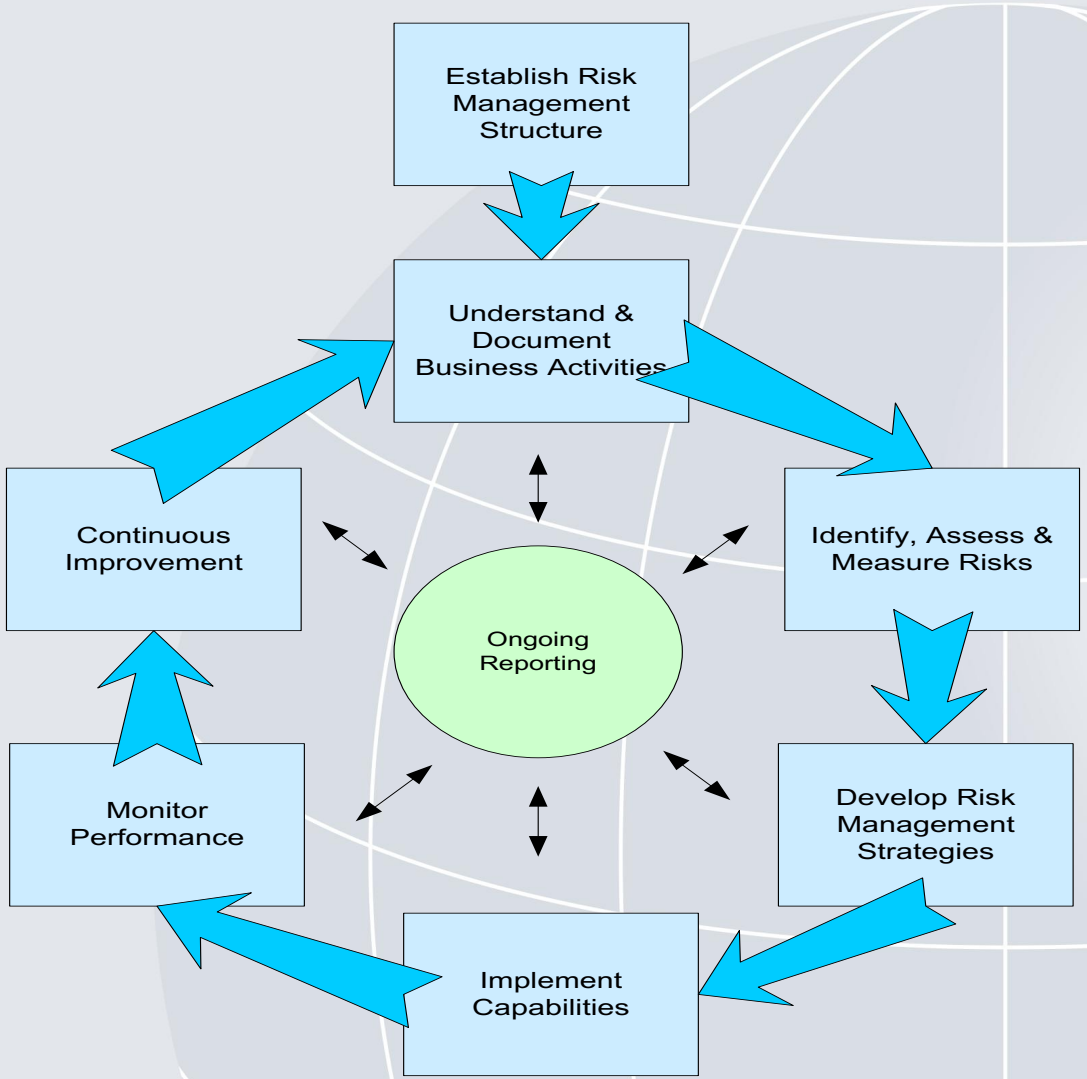
- The BCP focuses on the basic elements of Operational Continuity of the DMO: critical functions, key personnel, critical systems, alternate facilities and remote operation, order of command succession and delegation of authority tables, presents the development of procedures to guarantee operational continuity applied to all the spectrum of threats and emergencies that could affect the DMO

DMO Policy for the BCP

The DMO policy will be to:

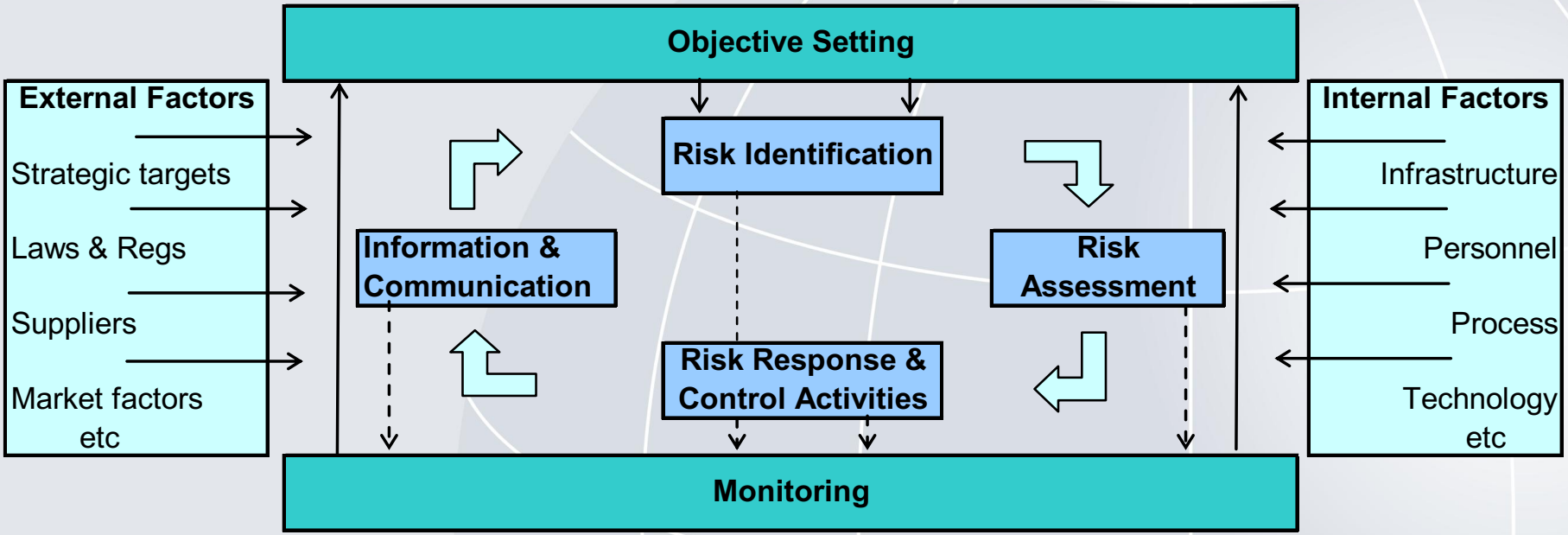
- perform a business impact analysis, and develop mitigation strategies, which will ensure the continuity of its business, operations and technology components in the event the existing environment is unavailable
- develop and maintain a comprehensive business continuity and disaster recovery plan (BCP/DRP) to ensure that essential/critical DMO activities are recoverable (business continuity planning and the BCP/DRP will be developed in accordance with international standards such ISO 22301)
- report the status of business continuity planning and the BCP/DRP annually to the Head of the Ministry of Finance

Six-Step BCP Framework for the DMO



Source: World Bank 2010

Example: Turkish Treasury



Source: Hakan Tokaç and Mike Williams (2013)

Six-step BCP Practical Framework

1. Document **business activities** and **critical processes and systems**
2. Undertake **business impact analysis** to assess probability and impact
3. Develop **BCP** (include 3rd parties)
4. **Implement** or **update** BCP
5. **Training** to imbed into the day-to-day operations of the the DMO
6. Regular (at least annual) **testing** and **updating**

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	Financial Loss Impact	Impact on Outputs or Budget Variance
Very-High	Loss of stakeholder confidence Loss of market confidence Loss of trust, e.g. from primary dealers Extensive media coverage High-level ministerial enquiry [or resignation]	Reported in government's financial statements Significant amount of time spent dealing with issue (i.e. greater than 30 person-days)	Significant delay in achieving outputs Significant debt service budget variance (i.e. greater than 10%)
High	Strained stakeholder relationships Temporary loss of market confidence Moderate media coverage Ministerial enquiry	Reported to minister Large amount of time spent dealing with issue (i.e. between 20 and 30 person-days)	Large delay in achieving outputs Large debt service budget variance (i.e. between 5% and 10%)
Medium	Increased stakeholder attention Market confidence not affected Minor, if any, media attention Major attention within ministry/DMO	Reported to the entity responsible for monitoring the DMO Moderate amount of time spent dealing with issue (i.e. between 10 and 20 person-days)	Moderate delay in achieving outputs Moderate debt service budget variance (i.e. between 3% and 5%)
Low	Stakeholder and market relationships intact No media coverage Internal ministry/DMO enquiry	Included in internal monthly reports Minimal amount of time spent dealing with issue (i.e. less than 10 person-days)	Little or no delay in achieving outputs Little or no debt service budget variance (i.e. less than 3%)

Source: World Bank 2010

Application to 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)

Application to 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 (4 x 4)

	Low Impact	Medium Impact	High Impact	Very-High Impact
Very-High Probability (almost certain)	VHpLi	VHpMi	VHpHi	VHpVHi
High Probability (probable)	HpLi	HpMi	HpHi	HpVHi
Medium Probability (possible)	MpLi	MpMi	MpHi	MpVHi
Low Probability (remote)	LpLi	LpMi	LpHi	LpVHi

Source: World Bank 2010

Example: Turkish Treasury (5 x 5)

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)

Business Continuity Planning

Normal Operations:
-Incident preparedness
-Maintain business continuity plan

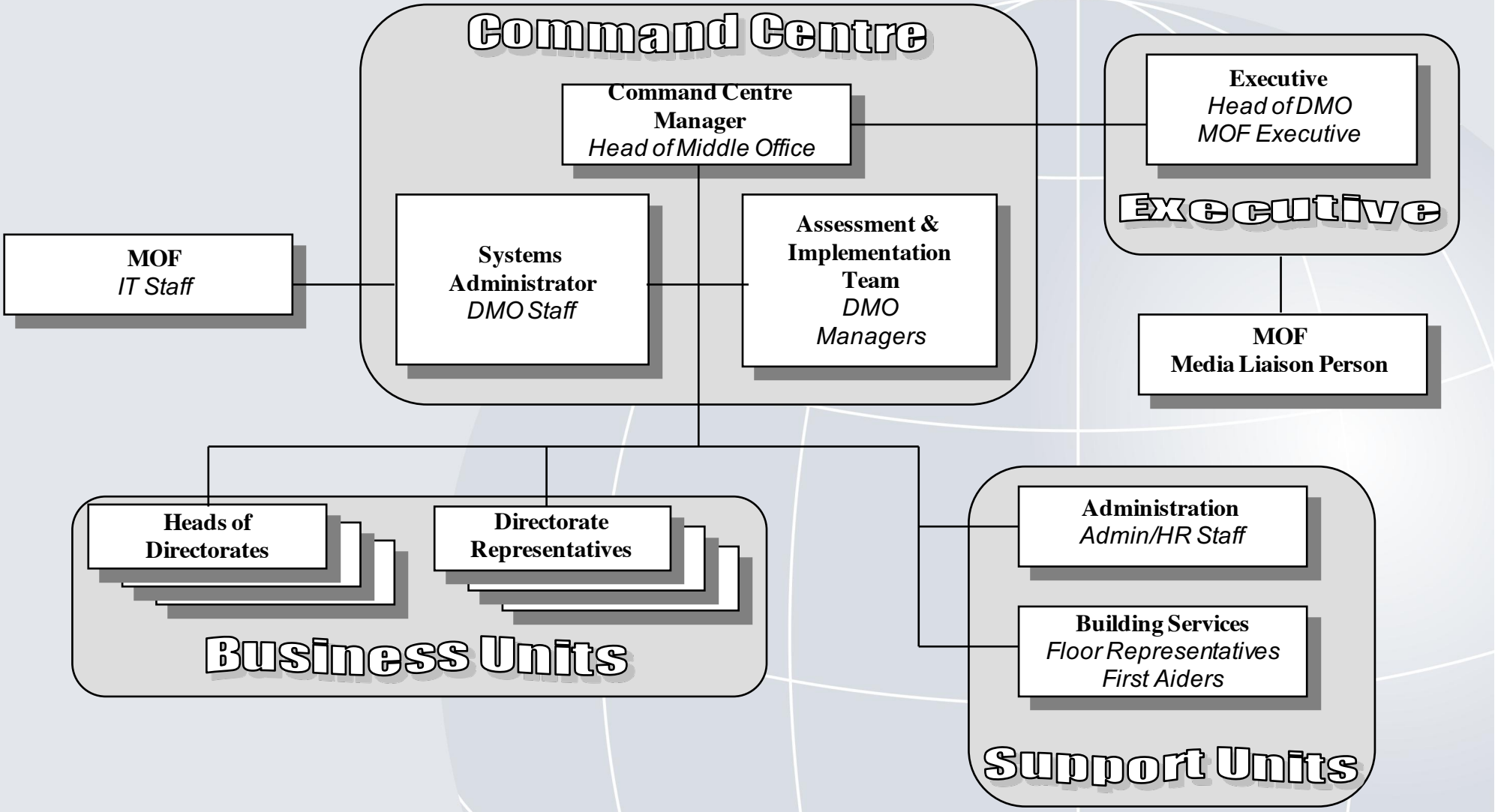
Incident

Emergency Response:
-Evacuation/containment
-Damage assessment
-Recovery decision

Business Recovery:
-Activate disaster recovery plan
-Survival level operations
-Escalation if necessary
-Primary site recommissioning

Post-incident Review

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

Wallet Card Side #1

Debt Management Office Contingency Pack

THIS DOCUMENT IS PRIVATE & CONFIDENTIAL

Staff should keep this document with them at all times

Issue 1 — 19 January, 2016

After Hours Emergencies

- **If you are in the building after hours and an evacuation is ordered**, ensure that a member of the Command Centre Team is informed.
- **If you are denied access** to the building when you arrive at work, go to the evacuation assembly area and await further instructions.
- **If you hear of a disaster affecting the building**, remain at home. Contact a member of the Command Centre Team if possible or wait to be contacted.

Floor Representatives

These staff coordinate the evacuation and ensure all staff and visitors get out.

Name	Floor	Ext.

Emergency Command Centre

Members of the Command Centre Team local to the incident will assemble at the following location:

Working Hours: Building Alarm

- Conclude phone calls
- Escort visitors to stairwell
- Assist persons with disabilities to evacuate
- Follow wardens' instructions
- Use fire-fighting equipment only if no danger is involved
- Assemble at evacuation point (see map below)
- DO NOT disperse. Await instructions from the Command Centre Team

If You Discover an Incident...

- **Fire**: Activate nearest fire alarm. Obtain an outside line and phone xxx. Give the operator exact location of premises and fire. Alert a DMO floor representative or the building manager. Evacuate to designated assembly area as shown below.
  DON'T use lifts, turn off lights, run, pass others on stairs
- **Bomb threat:** Follow instructions on Bomb Threat checklist. Alert police and chief warden. Any call must be treated as genuine until confirmed otherwise. When instructed, evacuate to designated assembly area as shown below taking personal belongings with you.
- **Suspicious package**: Refer to the "Suspicious letter or package" recognition points on the flip side of the Bomb Threat Card. Alert the building manager or police. Do not move the package.
- **Stranger in the office**: Ask them who they are and who they are there to see. If they cannot provide an explanation, alert building security or the police.
- **Flooding**: Alert the building manager. Move papers and disconnect nearby electrical equipment ONLY if safe to do so.

In all cases notify the Command Centre Team

Media Guidelines

❑

Building Locations

DMO	Tel:
Accountant General	Tel:
Central Bank	Tel:
Central Bank Alternate Site	Tel:
IT	Tel:

Earthquake

Working hours:

- Move away from windows and heavy equipment
- Shelter under solid furniture
- If fire breaks out, attempt to extinguish only if safe
- If instructed to vacate, follow evacuation procedures
- Follow instructions from Wardens, Security or Police

After hours:

- Attempt to contact the Command Centre Team
- Attempt to get to the office when possible
- Follow all Emergency Services directives and ensure the safety of your home and family

First Aid / Civil Emergency

The following staff have received training:

Name	Floor	Phone

Staff Relocation

Evacuation Assembly Point

Map of CBD

Building Services

Emergency Services

In an emergency (police / fire / ambulance) **Dial xxx**

Name	Role	Phone
	Building Manager	
	A-Hours / Security	

Wallet Card Side #2

Business Recovery Check List for <insert> Office

Commence this checklist ONLY when directed by the Command Centre Team

Issue 1 19 January, 2016

Recovery Organisation

- ▲ Follow all instructions of the Command Centre Team.
- ▲ DO NOT initiate any recovery activities without clearance from the Command Centre Team.
- ▲ DO NOT make any statements to the media. Refer media enquiries to the Command Centre Team.
- ▲ Any staff not immediately required for recovery purposes should return home and await instructions.
- ▲ Keep the Command Centre Team informed of your whereabouts.

If Evacuating the Building

Ensure the following items are taken:

- ❑ Phone lists, address books, client lists
- ❑ Mobile phone and charger
- ❑ Laptop
- ❑
- ❑

MOF/DMO Staff Contact Details

	Ext	Mobile	Home
DMO			
MOF Executive Team			
Admin / HR / Building Services			
Media Spokesperson			
IT			
Helpdesk			

Reference Documents

Item	Location
Bomb Threat Card	All Workstations
Emergency Evacuation Procedures	MOF
DMO BCP	DMO
IT BCP	IT Office
Central Bank BCP	Central Bank

Access to Systems

System	Access Method	Operational By	Data as at (date)
DRMS	Online IT	Present day + 1	Previous Thursday
IFMIS	Online IT	Present day + 1	Previous Thursday
Banking & Settlement	Online Central Bank	Present day	Present day
MS Office	Online IT	Present day + 1	Previous Thursday
Bloomberg	Online DMO	Present day	Present day

Post-Incident Check List

- ❑
- ❑
- ❑
- ❑
- ❑
- ❑
- ❑
- ❑

Phone Diversion Instructions

PABX

- ➢ Seize the main line (line 1) a dial tone will be heard OR
- ➢ Dial ?????

To activate an existing divert code

- ➢ Enter the divert code

To create new divert codes

- ➢ Dial ???
- ➢ Enter new divert code (???)
- ➢ Enter area code & phone number
- ➢ Wait for dial tone
- ➢ **To activate divert code**
- ➢ Enter your divert code

To finish operation

- ➢ Hang up
- ➢ Upon seizing the line again, interrupted dialtone is heard

To switch Call Diversion of

- ➢ Dial ???
- ➢ Hang up

Pre-set Divert Codes

- ➢ ??? Diverts to

External Contacts

Company	Name	Phone
Attorney General		
Central Bank		
IT		
Legal		
Bloomberg		

<insert> Office Staff

Name	Mobile	Home

Example: Colombia DGCPTN

Tarjeta Plan de Continuidad de Negocio

MINHACIENDA DGCPTN TODOS POR UN NUEVO PAÍS

ESTE ES UN DOCUMENTO
PRIVADO & CONFIDENCIAL

El personal debe llevar este documento consigo en todo momento

Versión 1.1 20 abril, 2015

Primeros auxilios y defensa civil

El botiquín de primeros auxilios y recursos de la defensa civil se encuentran en el parqueadero y cocina

Los siguientes funcionarios están capacitados en primeros auxilios:

- Maria del Pilar Bobadilla (3163), Mayerli Cuenca (3190), Diana Rocio Piratova (1145), Carlos Alberto Sanabria (1115).

Directorio de contactos clave

	Celular	Casa .
Director Crédito Público		
Pablo Cárdenas	3213150879	3021665
Subdirector de Financiamiento Interno		
Luis Alexander Lopez	3164114244	465 31 83
Subdirector de Operaciones		
Jorge Calderon	3104052770	6273173
Subdirección de Riesgo		
Andres Quevedo	3212306409	2183854
Arley Molano	3132403459	2226138
Diana Quiroga	3102033773	7575313

Punto de encuentro en caso de evacuación

En caso de una evacuación, favor dirigirse al punto de encuentro exterior:

- Parque Bolivia: Cra 10 con Calle 7

NO dispersarse hasta que se le instruya hacerlo

En caso de evacuar el edificio

Asegúrese de llevarse los siguientes artículos:

- Teléfonos celulares
- Documentos
- Dispositivos de almacenamiento electrónico (USBs, CDs, DVDs), que puedan tener información importante)

Teléfonos de emergencia

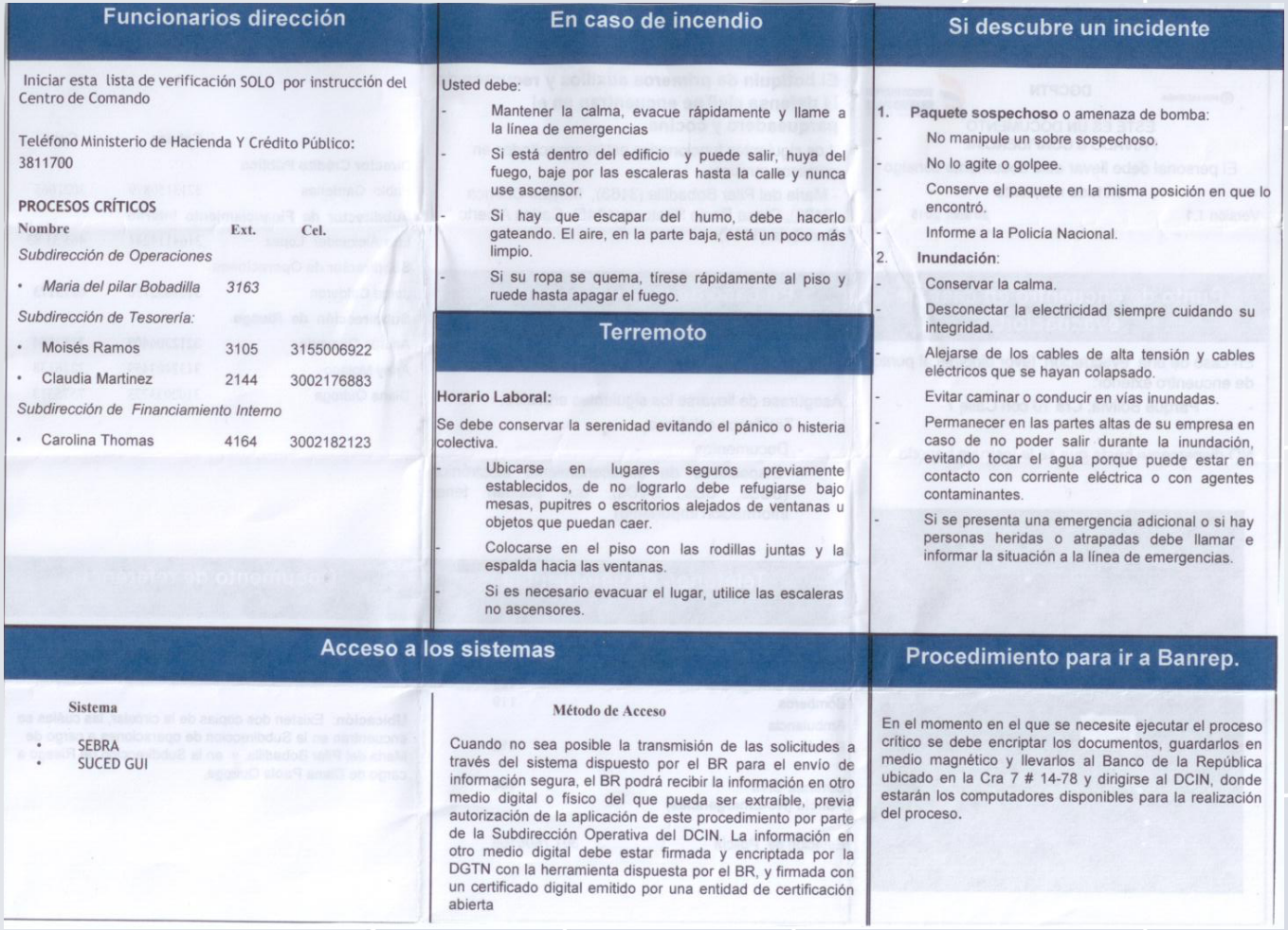
Teléfono de Servicios Emergencia	
Línea de emergencia	**123**
Bomberos	119
Ambulancia	
Policía	112
Defensa Civil	**144**
Policía (No-Emergencias)	
Estación de Policía	301 7605166

Documento de referencia

Ítem: CIRCULAR REGLAMENTARIA EXTERNA - DCIN – 308 del Banco de la República

Ubicación: Existen dos copias de la circular, las cuáles se encuentran en la Subdireccion de operaciones a cargo de Maria del Pilar Bobadilla, y en la Subdireccion de Riesgo a cargo de Diana Paola Quiroga.

Example: Colombia DGCPTN



Funcionarios dirección

Iniciar esta lista de verificación SOLO por instrucción del Centro de Comando

Teléfono Ministerio de Hacienda Y Crédito Público: 3811700

PROCESOS CRÍTICOS

Nombre	Ext.	Cel.
Subdirección de Operaciones		
• *Maria del pilar Bobadilla*	*3163*	
Subdirección de Tesorería:		
• Moisés Ramos	3105	3155006922
• Claudia Martinez	2144	3002176883
Subdirección de Financiamiento Interno		
• Carolina Thomas	4164	3002182123

En caso de incendio

Usted debe:

- Mantener la calma, evacue rápidamente y llame a la línea de emergencias
- Si está dentro del edificio y puede salir, huya del fuego, baje por las escaleras hasta la calle y nunca use ascensor.
- Si hay que escapar del humo, debe hacerlo gateando. El aire, en la parte baja, está un poco más limpio.
- Si su ropa se quema, tírese rápidamente al piso y ruede hasta apagar el fuego.

Terremoto

Horario Laboral:

Se debe conservar la serenidad evitando el pánico o histeria colectiva.

- Ubicarse en lugares seguros previamente establecidos, de no lograrlo debe refugiarse bajo mesas, pupitres o escritorios alejados de ventanas u objetos que puedan caer.
- Colocarse en el piso con las rodillas juntas y la espalda hacia las ventanas.
- Si es necesario evacuar el lugar, utilice las escaleras no ascensores.

Si descubre un incidente

1. **Paquete sospechoso** o amenaza de bomba:
   - No manipule un sobre sospechoso.
   - No lo agite o golpee.
   - Conserve el paquete en la misma posición en que lo encontró.
   - Informe a la Policía Nacional.
2. **Inundación**:
   - Conservar la calma.
   - Desconectar la electricidad siempre cuidando su integridad.
   - Alejarse de los cables de alta tensión y cables eléctricos que se hayan colapsado.
   - Evitar caminar o conducir en vías inundadas.
   - Permanecer en las partes altas de su empresa en caso de no poder salir durante la inundación, evitando tocar el agua porque puede estar en contacto con corriente eléctrica o con agentes contaminantes.
   - Si se presenta una emergencia adicional o si hay personas heridas o atrapadas debe llamar e informar la situación a la línea de emergencias.

Acceso a los sistemas

Sistema	Método de Acceso
• SEBRA • SUCED GUI	Cuando no sea posible la transmisión de las solicitudes a través del sistema dispuesto por el BR para el envío de información segura, el BR podrá recibir la información en otro medio digital o físico del que pueda ser extraíble, previa autorización de la aplicación de este procedimiento por parte de la Subdirección Operativa del DCIN. La información en otro medio digital debe estar firmada y encriptada por la DGTN con la herramienta dispuesta por el BR, y firmada con un certificado digital emitido por una entidad de certificación abierta

Procedimiento para ir a Banrep.

En el momento en el que se necesite ejecutar el proceso crítico se debe encriptar los documentos, guardarlos en medio magnético y llevarlos al Banco de la República ubicado en la Cra 7 # 14-78 y dirigirse al DCIN, donde estarán los computadores disponibles para la realización del proceso.

Case of México: TESOFE BCP/DRP

IT Data Center in Aquascalientes (500km north of Mexico City)

Bank of México

TESOFE

Alternate Data Center in TESOFE Building

Alternate Site in Legaria, Mexico City

Six Key Observations on BCP

1. There are a relatively small number of critical activities or processes in a DMO
   - **BCP can be simple and not expensive**
2. The critical systems used by a DMO are a DRMS, Auction System, Banking Systems, and Microsoft Office, particularly email and Excel
3. In the event of an incident requiring relocation of key staff, normally a small number of staff would be needed depending on the critical activities at the time of the incident

Six Key Observations on BCP ctd…

4. A DMO is normally very dependent on emails for communication within the DMO, other government agencies, and external parties
5. Two key external parties on which a DMO is highly dependent are normally
   - Central Bank
   - Accountant General (or Treasury)
6. There is often a need to review the IT backup policy as this can present a risk of loss of debt data depending on the frequency of the backups

Successful BCP Implementation

- Appoint a **BCP champion** *(from the middle office)* to oversee implementation of measures approved by senior management:
  - training program
  - raising awareness
  - introducing BCP requirement into SLAs or MOUs
  - developing control tools and mitigation strategies
  - developing reporting requirements
  - maintaining BCP and at least annual testing

Source: World Bank 2010

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/bcbs/index.htm]

- 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.oecd.org/site/sigma/publicationsdocuments/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://go.worldbank.org/GLNMQ6PVA0]

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/~/media/Uploads/documents/business_continuity_management.pdf
- Government of Canada (2012), **"A Guide to Business Continuity Planning"** http://www.gov.mb.ca/emo/home/bcont_e.pdf
- French General Secretary of Defense and National Security (2013), **"Guide pour Réaliser un Plan de Continuité D'Activité"** http://www.economie.gouv.fr/files/hfds-guide-pca-plan-continuite-activite-_sgdsn.pdf
- New Zealand Ministry of Civil Defence and Emergency Management (2006), **"Guide to the National Civil Defence Emergency Management Plan"** http://www.civildefence.govt.nz/memwebsite.nsf/Files/The-Guide-2009-revision/$file/The-Guide-v1.2-complete-web.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"** http://www.coso.org
- 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