Operational Risk Management and Business Continuity

Presentation by: Ian Storkey

March 17, 2011
ORM & BCP – Why Necessary?

**ORM Govt Cases**
- Orange County (1994)
- Hammersmith & Fulham Council (1989)

**BCP Facts**
- Over one third of businesses that suffer a significant, though not necessarily catastrophic, business interruption are no longer in business within two years of the event.

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.

Mexico, Sep 1985  
Chile, Feb 2010
ORM & BCP – Why Not Addressed?

- Mainly executive neglect:
  - “it won’t happen to me” is alive and well
  - inadequate resource allocation
  - low priority
  - responsibility delegated
  - project versus program
  - relative lack of regulatory pressure

- How well prepared is your Treasury?
  - do you have a full business continuity and disaster recovery plan?
  - has the BCP been tested in the last 12 months?
  - is your BCP managed by IT or risk management?
  - is business continuity viewed within an ORM framework?

Central Banks are normally better prepared than Ministry of Finance, have a recovery infrastructure and alternate site, and regularly test – maybe the central bank can assist the Ministry of Finance.
Operational Risk Management

The risk of loss resulting from inadequate or failed internal processes, people and systems or from external events

- definition explicitly includes legal risk, but excludes strategic and reputation risk
- has been applied to government debt management in publication by World Bank

Source: Basel II (June 2004)
## Operational Risks for Treasury Management

### Infrastructure and Technology Failures

<table>
<thead>
<tr>
<th>Power failure</th>
<th>Hardware failure</th>
<th>Sabotage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data corruption including viruses</td>
<td>LAN/WAN/Intranet/ Internet failure</td>
<td>Internal flood (sprinklers, pipes)</td>
</tr>
<tr>
<td>Voice network failure</td>
<td>Theft of equipment</td>
<td>Theft of data/information</td>
</tr>
<tr>
<td>Poor maintenance</td>
<td>Accidental damage</td>
<td></td>
</tr>
</tbody>
</table>

### Incidents Where Access to Premises is Denied

<table>
<thead>
<tr>
<th>Flooding or a fire concern</th>
<th>Health and safety violation</th>
<th>Hazardous chemicals accident</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gas or chemical leak</td>
<td>Industrial action or riot</td>
<td>Bomb or terrorist threat</td>
</tr>
<tr>
<td>Building fire or explosion</td>
<td>Internal/external flood</td>
<td>Sabotage or terrorism</td>
</tr>
</tbody>
</table>

### Key Service Providers or Resource Failures Dependencies

<table>
<thead>
<tr>
<th>Failure of key service providers (telephone, internet, banking etc)</th>
<th>Third party providers (Central Bank and other outsourced operations)</th>
<th>Impact of incident on critical teams or groups (travel, food poisoning, group incident)</th>
</tr>
</thead>
</table>
## Operational Risks for Treasury Management

<table>
<thead>
<tr>
<th><strong>Staff, Management and Related Human Failures</strong></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Human error (which may be due to poor training or inadequate supervision)</td>
<td>Poor training or inadequate supervision (which may lead to human error or execution of unauthorized transactions)</td>
<td>Failure to follow code of conduct or conflict of interest guidelines</td>
</tr>
<tr>
<td>Lack of policy guidance (which may lead to poor decisions or unauthorized activities)</td>
<td>Poor understanding of risk environment (which may lead to unnecessary or unknown risks)</td>
<td>Poorly specified delegations (which may lead to execution of unauthorized transactions)</td>
</tr>
<tr>
<td>Failure to follow or adhere to administrative practices (which may lead to processing errors)</td>
<td>Key person risk (which may lead to human error when key person is absent)</td>
<td>Fraudulent, corrupt or dishonest practices (which may lead to financial loss and political embarrassment)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Failure to Meet Statutory, Legal, Human Resources and Other Obligations</strong></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Legal/statutory obligations (e.g. compliance with loan agreements)</td>
<td>Management directives (e.g. internal policies and procedures)</td>
<td>Procedures manuals and delegated authorities</td>
</tr>
<tr>
<td>Reporting obligations (e.g. to higher authorities and international institutions)</td>
<td>Contractual obligations (e.g. debt service obligations)</td>
<td>Health and safety regulations (e.g. national workplace laws or regulations)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Major Natural and Regional Disasters</strong></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Earthquake</td>
<td>Severe flooding</td>
<td>Tsunami</td>
</tr>
<tr>
<td>Volcanic eruption</td>
<td>Severe fires</td>
<td>Civil disturbance or terrorism</td>
</tr>
</tbody>
</table>

*Source: World Bank 2010*
Six-Step ORM Framework

Establish Risk Management Structure

Understand & Document Business Activities

Identify, Assess & Measure Risks

Develop Risk Management Strategies

Implement Capabilities

Monitor Performance

Continuous Improvement

Ongoing Reporting

Source: World Bank 2010
<table>
<thead>
<tr>
<th>Probability</th>
<th>Low Impact</th>
<th>Medium Impact</th>
<th>High Impact</th>
<th>Very-High Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very-High Probability (almost certain)</td>
<td>VHpLi</td>
<td>VHpMi</td>
<td>VHpHi</td>
<td>VHpVHi</td>
</tr>
<tr>
<td>High Probability (probable)</td>
<td>HpLi</td>
<td>HpMi</td>
<td>HpHi</td>
<td>HpVHi</td>
</tr>
<tr>
<td>Medium Probability (possible)</td>
<td>MpLi</td>
<td>MpMi</td>
<td>MpHi</td>
<td>MpVHi</td>
</tr>
<tr>
<td>Low Probability (remote)</td>
<td>LpLi</td>
<td>LpMi</td>
<td>LpHi</td>
<td>LpVHi</td>
</tr>
</tbody>
</table>

Source: World Bank 2010
## Impact Guidelines

<table>
<thead>
<tr>
<th>Assessment of Impact</th>
<th>Reputational Impact</th>
<th>Financial Loss Impact</th>
<th>Impact on Outputs or Budget Variance</th>
</tr>
</thead>
</table>
| **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/DMU | Reported to the entity responsible for monitoring the DMU  
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/DMU 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*
**Business Continuity Planning**

**DMO/Treasury Risks**

**Operational Risks**

**Financial Risks**

**Business Risks**

**Risks Addressed by BCP**

**Incident**

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

**Normal Operations:**
- Incident preparedness
- Maintain business continuity plan

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

**Post-incident Review**

**Normal Operations:**
- Incident preparedness
- Maintain business continuity plan

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

**Post-incident Review**
Six-step BCP/DRP Framework

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

- Appoint an **ORM/BCP champion** to oversee implementation of measures approved by senior management:
  - training program
  - raising awareness
  - introducing ORM/BCP into service level agreements
  - developing control tools and mitigation strategies
  - developing reporting requirements
  - maintaining ORM/BCP and annual testing

Source: World Bank 2010
References


II SEMINARIO LATINOAMERICANO SOBRE GESTIÓN DE TESORERÍAS PÚBLICAS 2011

México
16 - 18 Marzo 2011