Operational Risk Management (ORM) and Business Continuity Plans (BCP)

Ian Storkey, Consultant
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 Ministry?**
  - 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 unit?
  - 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...
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 Debt Management

### Infrastructure and Technology Failures

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Power failure</td>
<td>Hardware failure</td>
<td>Sabotage</td>
</tr>
<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>Incident</th>
<th>Health and safety violation</th>
<th>Hazardous chemicals accident</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flooding or a fire concern</td>
<td></td>
<td></td>
</tr>
<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>Incident</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, pandemic)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failure of key service providers (telephone, internet, banking etc)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Operational Risks for Debt Management

<table>
<thead>
<tr>
<th>Staff, Management and Related Human Failures</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>
</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>
</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>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Failure to Meet Statutory, Legal, Human Resources and Other Obligations</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>
</tr>
<tr>
<td>Reporting obligations (e.g. to higher authorities and international institutions)</td>
<td>Contractual obligations (e.g. debt service obligations)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Major Natural and Regional Disasters</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Earthquake</td>
<td>Tsunami</td>
</tr>
<tr>
<td>Volcanic eruption or landslide</td>
<td>Severe fires</td>
</tr>
</tbody>
</table>
Six-Step ORM Framework

1. Establish Risk Management Structure
2. Understand & Document Business Activities
3. Identify, Assess & Measure Risks
4. Develop Risk Management Strategies
5. Implement Capabilities
6. Continuous Improvement
7. Monitor Performance
8. Ongoing Reporting
Example: Turkey

Source: Hakan Tokaç and Mike Williams (2011)
# Probability and Impact

<table>
<thead>
<tr>
<th></th>
<th>Low Impact</th>
<th>Medium Impact</th>
<th>High Impact</th>
<th>Very-High Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Very-High</strong></td>
<td>VHpLi</td>
<td>VHpMi</td>
<td>VHpHi</td>
<td>VHpVHi</td>
</tr>
<tr>
<td>Probability</td>
<td>(almost</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>High</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Probability</td>
<td>(probable)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Medium</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Probability</td>
<td>(possible)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Low</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Probability</td>
<td>(remote)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Example: Turkey

<table>
<thead>
<tr>
<th>Likelihood level of risk</th>
<th>Impact level of risk</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Insignificant</td>
</tr>
<tr>
<td>Very Low</td>
<td>1</td>
</tr>
<tr>
<td>Low</td>
<td>1</td>
</tr>
<tr>
<td>Medium</td>
<td>2</td>
</tr>
<tr>
<td>High</td>
<td>2</td>
</tr>
<tr>
<td>Very High</td>
<td>2</td>
</tr>
</tbody>
</table>

Source: Hakan Tokaç and Mike Williams (2011)
## 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%) |
Business Continuity Planning

Risks Addressed by BCP

DMO Risks
Operational Risks
Financial Risks
Business Risks

Normal Operations:
- Incident preparedness
- Maintain business continuity plan

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

Normal Operations:
- Incident preparedness
- Maintain business continuity plan

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:
Disaster Recovery

Command Centre

- Command Centre Manager
  - Head Middle Office
- Business Systems
  - DMO
  - IT Staff
- Assessment & Implementation Team
  - Key DMO Managers

Executive

- Head DMO
- MoF Executive

MoF Media Liaison Person

Support Units

- Administration
  - Admin Staff
- Building Services
  - Floor Wardens
  - First Aiders

Business Units

- Heads of Department
- Department Representatives

MoF Business Systems

IT Staff
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 ministry of finance
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
ORM and BCP Implementation

• Appoint an **ORM/BCP champion** to oversee implementation of measures approved by senior management:
  – introduce training program
  – raise awareness across DMO and MoF
  – introduce ORM/BCP into service level agreements
  – develop control tools and mitigation strategies
  – create redundancy and recovery strategies
  – develop reporting requirements
  – maintain ORM/BCP and annual/regular testing
References


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

