Business Continuity and Risk Management

Ken Kaberia
Principal BCM Officer, Enterprise Risk
Safaricom Limited
What does Business Continuity mean?
Business Continuity Management - Definition

“Business Continuity Management is a holistic business approach that includes policies, standards, frameworks and procedures for ensuring that specific operations can be maintained or recovered in a timely fashion in the event of disruption. Its purpose is to minimise the operations, financial, legal, reputational and other material consequences arising from disruption”

-Central Bank of Kenya

“Business Continuity Management is a holistic management process that identifies potential impacts that threaten an organization and provides a framework for building resilience and the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value creating activities”

-Business Continuity Institute
Business Continuity Management (Simply Put)

– Identify threats to the organization
– Identify the impacts to your business operations that those threats, if realized might cause.
– Build resilience to ensure that the organization can respond immediately and effectively to a major incident.
What is Risk Management?

- Operational
- Reputational
- Strategic
- Compliance
- Information Security
- Malicious
- Financial

- Control Assessment
- Reporting
- Review risks regularly

- Monitor and communicate

- Assess Risk

- Implement strategies to minimize downside

- Strategies
  - Transfer
  - Retain/accept
  - Avoid
  - Reduce

- Critical
- High
- Medium
- Low
Risk Management tool?

3 WAYS TO DEAL WITH RISK

Managing Risks
Benefits from ERM

- Support Objectives
- Improve Earnings and Cash Flow
- Manage Growth
- Capture Opportunities

- Business Continuity
- Reduce Losses
- Lower Insurance Costs

- Purchase Insurance and Cover Risks
- Outsourcing

- ERM Approach
  - Optimizing Risk
  - Advanced Risk Management
  - Managing Risk
  - Defensive Risk Management
  - Transferring Risk
BCM as per BS25999 Standard

BCM MANAGEMENT LIFECYCLE

- Business Impact Analysis and Risk assessment
- Strategy Formulation
- Plans Development
- Plans Testing
- Training and Awareness
1

RISK ASSESSMENT AND BIA
( BUSINESS IMPACT ASSESSMENT)
# Risk assessment – Format?

<table>
<thead>
<tr>
<th>IMPACT</th>
<th>Financial Loss (loss of sales, unforeseen costs, legal liabilities, fraud)</th>
<th>Damaged Reputation (negative publicity,)</th>
<th>Any Other Ways</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ksh 500M +</td>
<td>Extensive negative publicity</td>
<td>Extremely serious impact</td>
<td>1</td>
</tr>
<tr>
<td>Ksh 50-500M</td>
<td>Any negative publicity</td>
<td>Very serious impact</td>
<td>2</td>
</tr>
<tr>
<td>Ksh 5-50M</td>
<td>Any publicity</td>
<td>Serious impact</td>
<td>3</td>
</tr>
<tr>
<td>Ksh 0.5-5M</td>
<td>No publicity</td>
<td>Minor impact</td>
<td>4</td>
</tr>
<tr>
<td>Ksh 0-0.5M</td>
<td>No publicity</td>
<td>No significant impact</td>
<td>5</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>LIKELIHOOD</th>
<th>Rare</th>
<th>Unlikely</th>
<th>Possible</th>
<th>Likely</th>
<th>Certain</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verbal Description</td>
<td>Extraordinary event might occur once every 5yrs</td>
<td>Possibly once a year</td>
<td>Might occur once a quarter</td>
<td>Might occur once a month</td>
<td>Is expected once a week</td>
</tr>
</tbody>
</table>

![Risk Assessment Matrix](image-url)
## Risk assessment – Threat versus Location

<table>
<thead>
<tr>
<th>Threat</th>
<th>Loc 1</th>
<th>Loc 2</th>
<th>Loc 3</th>
<th>Loc 4</th>
<th>Loc 5</th>
<th>Loc 6</th>
<th>Loc 7</th>
<th>Loc 8</th>
<th>Loc 9</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Security</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1. Civil disorder</td>
<td>LOW</td>
<td>MED</td>
<td>MED</td>
<td>LOW</td>
<td>LOW</td>
<td>MED</td>
<td>MED</td>
<td>LOW</td>
<td>LOW</td>
</tr>
<tr>
<td>2. Sabotage/Vandalism</td>
<td>MED</td>
<td>HIGH</td>
<td>MED</td>
<td>MED</td>
<td>LOW</td>
<td>MED</td>
<td>MED</td>
<td>MED</td>
<td>LOW</td>
</tr>
<tr>
<td>3. Bomb threats/Terrorism</td>
<td>HIGH</td>
<td>CRITICAL</td>
<td>MED</td>
<td>MED</td>
<td>LOW</td>
<td>LOW</td>
<td>LOW</td>
<td>LOW</td>
<td>LOW</td>
</tr>
<tr>
<td>4. Kidnap &amp; ransom</td>
<td>LOW</td>
<td>LOW</td>
<td>LOW</td>
<td>LOW</td>
<td>LOW</td>
<td>LOW</td>
<td>LOW</td>
<td>LOW</td>
<td>LOW</td>
</tr>
<tr>
<td>5. Transportation mishaps</td>
<td>LOW</td>
<td>LOW</td>
<td>LOW</td>
<td>MED</td>
<td>LOW</td>
<td>LOW</td>
<td>LOW</td>
<td>LOW</td>
<td>LOW</td>
</tr>
<tr>
<td><strong>Natural Disasters</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6. Fire</td>
<td>LOW</td>
<td>MED</td>
<td>MED</td>
<td>LOW</td>
<td>LOW</td>
<td>LOW</td>
<td>LOW</td>
<td>LOW</td>
<td>LOW</td>
</tr>
<tr>
<td>7. Flood</td>
<td>LOW</td>
<td>MED</td>
<td>LOW</td>
<td>LOW</td>
<td>LOW</td>
<td>LOW</td>
<td>LOW</td>
<td>LOW</td>
<td>LOW</td>
</tr>
<tr>
<td>8. Earthquake</td>
<td>MED</td>
<td>MED</td>
<td>LOW</td>
<td>LOW</td>
<td>MED</td>
<td>LOW</td>
<td>LOW</td>
<td>LOW</td>
<td>MED</td>
</tr>
<tr>
<td>9. Volcanic eruption</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>MED</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Technical failures</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
STRATEGY FORMULATION/GAPS IDENTIFIED
Business Impact Assessment

- Business unit & key processes
- Recovery time and point objective RTO/RPO
- Applications and other resources
- Impact/Criticality
Business Impact Assessment

- Business unit & key processes
- Recovery time and point objective RTO/RPO
- Applications and other resources
- Impact/Criticality
- Current mitigations
- Additional mitigations
- Budget required
DEVELOPING AND IMPLEMENTING A BCM RESPONSE
BCM Response

- Current mitigations
- Additional mitigations
- Budget required

- Implementation timelines and tracking
- Does it work?
TESTING AND MAINTAINING BCM
Why Test our plans?

- ** Validates** the BCP/DRP plans
- Generates **confidence** in the process
- Detects required **changes**
- **Trains** participants thereby improving recovery times
- **Reduces stress** during a real crisis
- Eliminates **inter-plan confusion** – all stakeholders work through the scenario together
Various types of testing available
Choose the type that suits your organisation best but ensure that it thoroughly tests the plans prepared.
TRAINING AND AWARENESS
Types of training

- Conferences
- Internal workshops
- Testing
- Awareness campaigns
- Quizzes
- Posters
- Intranet
CRISIS MANAGEMENT & COMMUNICATION
Categories of incidents

- Event: Non-routine action, covered by business plan.
- Incident: Local or short-term effects.
- Crisis: Wider or long-term effects, ongoing implications for the business.
- Disaster: Crisis cannot be managed for extended periods; normal business stopped.
Why a crisis management team?

• clear and co-ordinated response

• through a determined chain of command

• in a safe and responsible manner

• The Crisis Team will mobilise to manage the crisis situation, and will help to organise and control the recovery process
Business Continuity Elements

Emergency Response
“Processes & procedures” that are implemented throughout the organization to ensure appropriate immediate actions are taken and the crisis alert communicated.

Crisis Management
Key actions to build crisis management capability, and a framework to effectively manage a crisis, supported by best practice checklists and templates.

Business Continuity Plan (BCP)/ Disaster Recovery Plans (DRP)
A BCP includes planned actions to recover office infrastructure, process, systems and office accommodation back to an acceptable level within an agreed time scale.
How prepared are you?