Introduction to Business Continuity Management

Submitted by: DHL
Introduction to Business Continuity Management

March 2014

Martin Sun
Head of Security

2013 BCM plan targeting NFE roll-out countries and top 50 stations

<table>
<thead>
<tr>
<th>BCM Policy</th>
<th>Announced globally on January, 24th 2013</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provision of Resource</td>
<td>CT &amp; Station has appointed a BCM nominee with appropriate seniority to be accountable for implementing BCM</td>
</tr>
<tr>
<td>IMT</td>
<td>Station has formed an Incident Management Team (IMT) with deputies for all key functions</td>
</tr>
<tr>
<td>Business Analysis</td>
<td>Station has identified activities (operations) that support its key products and services and its priorities for recovery of critical activities</td>
</tr>
<tr>
<td>BIA Risk Assessment</td>
<td>Station has completed a business impact analysis and has identified and documented the site's threats</td>
</tr>
<tr>
<td>Determining Choices</td>
<td>Station has determined how it will recover each critical activity within its recovery time objective (RTO), including the resources required for resumption</td>
</tr>
<tr>
<td>Determining BCP Strategy</td>
<td>Station to create Business Continuity Plans (BCP) for all possible risks that could affect critical operations and the BCP’s are to detail how to manage the incident and how it will recover its activities</td>
</tr>
<tr>
<td>BCP’s</td>
<td>Station has ensured that its BCP arrangements are reviewed and documented at planned intervals</td>
</tr>
<tr>
<td>Maintaining and Reviewing</td>
<td>Station has ensured that its BCP arrangements are reviewed and documented at planned intervals</td>
</tr>
<tr>
<td>Testing and Exercising</td>
<td>Station IMT has successfully carried out 3 table top exercises in the past 12 months and any lessons learnt have been incorporated into future plans</td>
</tr>
</tbody>
</table>
What is Business Continuity Management?

The uninterrupted availability of resources necessary to run your operation at a level acceptable to the Incident Management Team.

What is Business Continuity?

The strategic and tactical capability of an organisation to plan for and respond to incidents and business disruptions in order to continue business operations at an acceptable predefined level.

What is Business Continuity management?

A holistic management process that identifies potential threats to an organisation and the impacts to business operations those threats, if realised, might cause, and which provides a framework for building organisational resilience with the capability of an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities.

Source: BSI;ISO 22301:2012
BCM supporting the 3 bottom lines

Identifying and achieving common global operational risk standards is becoming increasingly important in order to drive improvement in DGF’s three bottom lines

Provider of Choice
Customer demand in resilient and secure networks ISO 22301

Investment of Choice
Reductions in employee workplace accident costs and liability OHSAS 18000

Bottom Lines

Employer of Choice
A safe and secured workplace environment OHSAS 18000 & ISO 22301

Business Continuity management

What is ISO 22301?
A system that can be used to assess an organisation's ability to meet its own business continuity needs and obligations by providing the necessary tools to protect and help the organisation during a crisis situation.

Business Continuity Management System
Objectives of BCM

1. Minimised potential economic loss
2. Reduced legal liability
3. Reduced disruption to normal operations
4. Ensured orderly recovery
5. Reduced reliance on key personnel
6. Ensured safety of personnel and customers
7. Minimised decision making during a disaster

Business Impact Analysis (BIA)

Evaluate:
1. Critical operations for the business
2. Determine tolerable downtime
3. Determine the resources for recovery
Threats to Business Continuity

Physical
- Natural catastrophe: Typhoon, Earthquake, Flood
- Malicious Damage: Fire, Arson, Vandalism
- Infectious Disease outbreak: SARS, Flu Pandemic

Technical
- Utility Disruption: Electricity, Water, Telecommunications
- Equipment Failure
- Hackers obtaining database and using it for identity theft
- Computer Virus Outbreak

Emotional
- Employee strike, disgruntled employees
- Loss of key employees, suppliers and customers
- Office pool winning the lottery
- Mass resignation

Risk Analysis & Review

- Identify existing and potential risks and threats the operation is exposed to.
- Assign ranking to each category with estimate of duration
- Determine which category to be examined further for countermeasures to be established to mitigate the risk
### Risk Analysis & Review – Threats Table

<table>
<thead>
<tr>
<th>Probability</th>
<th>Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>5 (Critical): Very likely the risk will occur</td>
<td></td>
</tr>
<tr>
<td>4 (Serious): Likely the risk will occur</td>
<td></td>
</tr>
<tr>
<td>3 (Moderate): Occasionally the risk will occur</td>
<td></td>
</tr>
<tr>
<td>2 (Minor): Unlikely the risk will occur</td>
<td></td>
</tr>
<tr>
<td>1 (Negligible): Very unlikely the risk will occur</td>
<td></td>
</tr>
</tbody>
</table>

#### Risk Matrix – Probability Severity Levels

- Accidents
- Aircraft accidents
- Airport closure
- Robbery
- Bankruptcy
- Berserk employee
- Bomb threat
- Boycott
- Business scandal
- Chemical spill
- Civil unrest
- Class action
- Collapse of structures
- Computer/ IT failure
- Denial of entry
- Death (employee or customer)
- Drug abuse
- Earthquake
- Executive succession/ departure
- Explosion
- Extortion
- Fire
- Flood
- Harbour/ port blockage
- Hijacking
- Infectious disease outbreak
- Kidnap/ ransom
- Landslide
- Lawsuit
- Layoff
- Libel/ slander
- Litigation
- Malicious damage
- Murder
- Negative media exposure
- Packaging problems
- Personal threats
- Pollution
- Political upheaval
- Product contamination
- Professional liability
- Regulatory changes
- Rumour and innuendo
- Sabotage
- Sexual harassment
- Storm
- Suicide
- Terrorism
- Theft
The BCMS

Corporate commitment, Internal issues, Interested parties, BCMS scope, BC Policies and objectives, Organisational risk, Resources, Responsibilities and authority, Competence, Awareness, Communication, Documented information

Monitoring measurement, Analysis, Evaluation, Internal Audit, Management review

Actions to address nonconformities, Continual improvement

Continual Improvement of BCMS

Interested parties

Establish (PLAN)

Maintain & Improve (ACT)

Monitor & review (CHECK)

Implement & Operate (DO)

Interested parties

Managed BC

Business Continuity Management System and PDCA

Business Continuity management System
Project Planning

2013 BCM plan targeting NFE roll-out countries and top 50 stations

<table>
<thead>
<tr>
<th>BCM Policy</th>
<th>Announced globally on January 24th 2013</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provision of Resource</td>
<td>CT &amp; Station has appointed a BCM nominee with appropriate seniority to be accountable for implementing BCM</td>
</tr>
<tr>
<td>IMT</td>
<td>Station has formed an Incident Management Team (IMT) with deputies for all key functions</td>
</tr>
<tr>
<td>Business Analysis</td>
<td>Station has identified activities (operations) that support its key products and services and its priorities for recovery of critical activities</td>
</tr>
<tr>
<td>BIA Risk Assessment</td>
<td>Station has completed a business impact analysis and has identified and documented the risks</td>
</tr>
<tr>
<td>Determining Choices</td>
<td>Using the Risk Assessment to document the station has, for each of its critical activities, identified available risk solutions</td>
</tr>
<tr>
<td>Determining BCP Strategy</td>
<td>Station has determined how it will recover each critical activity within its recovery time objective (RTO), including the resources required for resumption</td>
</tr>
<tr>
<td>BCP's</td>
<td>Station to create Business Continuity Plans (BCPs) for all possible risks that could affect critical operations and the BCP's are to detail how to manage the incident and how it will recover its activities</td>
</tr>
<tr>
<td>Maintaining and Reviewing</td>
<td>Station has ensured that its BCP arrangements are reviewed and documented at planned intervals</td>
</tr>
<tr>
<td>Testing and Exercising</td>
<td>Station IMT has successfully carried out 3 table top exercises in the past 12 months and any lessons learnt have been incorporated into future plans</td>
</tr>
</tbody>
</table>
The Business Continuity Management (BCM) Policy for DHL Global Forwarding establishes common principles of business continuity planning (development), implementation, exercise and maintenance. This document has been designed to provide the BU with one universal frame document in order to help our company to safeguard its human and financial assets and those entrusted to us by our customers as well as company reputation. This BCM Policy ensures adherence to Group’s guidelines and international standards and principles.

Scope
DHL Global Forwarding (DGF) shall be prepared for scenarios that may result in any disruption to services and processes and includes, but is not limited to, natural disasters, terrorist incidents, power outage, political unrest, general system failure or data corruption, etc.

The GFFB has directed that the BCM capability has to be established DGF-worldwide as a whole. This policy contains basic guidelines and methodology for BCM and applies to all staff, stations, visitors and sub-contractors.

This policy is applicable to the entire Business Unit DHL Global Forwarding.

Country Implementation Team / Incident Management Team

Sample structure; should be adapted according to country reality
Team selection and developing a plan

- Security - BCM Coordinator
- Gather support/commitment from senior management on implementation of BCM
- Appoint Implementation Team
- Develop Implementation framework/timeline
- Select team – establish roles and responsibilities of Incident Management Team
- Develop Plan

IMPLEMENT OUTLINE

BCMS Documentation

Typical Hierarchy

- Level 1: Overview of the organization and its approach to business continuity
- Level 2: Policy
- Level 3: Procedures
- Level 4: Operational documentation
- Records

BSI
IMPLEMENT OUTLINE

Procedures and Processes Required

• 4.2.2 Legal and regulatory requirements procedure
• 7.4 Communication procedure
• 8.4.1 Documented Procedure for managing a disruptive incident.
• 8.4.2 Documented Procedure for a response to a disruptive incident.
• 8.4.3 Warning and communication procedure
• 8.4.4 Documented procedures for BC Plans
• 8.4.5 Documented procedures for recovery to business as usual

bsi.

IMPLEMENT OUTLINE

Procedures and Processes Required

• 9.1.1 Monitoring performance procedure
• 9.2 Internal audit procedure
• 7.5.2 Creating and updating documented information: process
• 8.1 Risk control: process
• 8.2.1, 8.2.2, 8.2.3: BIA and Risk Assessment: documented process
• 8.4.4 BCP Activation and stand down: process

bsi.
Operate & Assess the System

Process Planning "Turtle Diagram"

- **With what?**
  - Resources

- **With Who?**
  - Personnel

- **Inputs**
  - From whom/where

- **Process**
  - (specific value added activities)

- **Outputs**
  - To whom/where

- **How done?**
  - Methods/Documentation

- **What results?**
  - Performance indicators

---

Operate & Assess the System

**Resumption of Activities**

- Normal activity
- Incident
- Time after which irrevocable damage is done to the organization
- Objective to resume activity
- Time to resume activity
- Time to resume normal levels of operation

---
Operate & Assess the System

Approaches to Business Impact Analysis (BIA)

- There is no single "right" way to conduct a BIA
- Any method that satisfies 8.2 is acceptable
- The BIA method may offer either
  - One BIA technique for universal use
  - A selection of techniques together with guidance on selecting one appropriate to the needs of specific activities (e.g., a BIA technique suited to IT or HR activities may not be equally suitable for IT or HR)
- Following slides illustrate a variety of BIA techniques

Impact Analysis

Impact can be quantitative or qualitative:
- Loss of key personnel
- Loss of physical assets
- Loss of information
- Disruption of service
- Violation of law, penalties
- Brand image, reputation, credibility
- Financial/revenue
- Customers, suppliers, partners
- Environmental/H&S

bsi.
Operate & Assess the System

BIA Report – Example Headings

- Executive Summary
- BIA Method Summary
- BIA by Department / Process
  - Operations
  - R&D
  - Finance
  - Sales & Marketing
  - HR
  - Vendor Management
  - Compliance and Risk
- Summary of Critical Activities and Impacts

Analyses impact of disruption of critical activities that support key products and services which, themselves, are of course cross-functional.

Operate & Assess the System

Risk Assessment

- Identify risks to prioritized activities, processes, resources, suppliers
- What are the threats and vulnerabilities?
- What are the probabilities of an incident?
- What treatments must be put in place to achieve the BC objectives?
Operate & Assess the System

Risk Assessment

- Threats
  - Civil unrest, labor action, fuel shortage, staff shortage
- Vulnerabilities
  - Unprotected perimeter, un-reviewed contracts, limited backup fuel storage, single source staff provider
- Probabilities
  - Estimated in percentage, likelihood of occurrences in a year, weighting factors such as industry sector or location

Operate & Assess the System

BCP

- BCP must be documented
- The BCP must contain:
  - Roles and responsibilities
  - Invocation and standing down
  - Incident management
  - Contact information
  - Communications
  - How prioritized activities will continue or be recovered
BCM Exercising

- Organization must conduct exercises and tests with defined aims and objectives and that minimize the risk of disruptions.
- We must produce post-exercise reports with outcomes and recommended improvements
- Exercises
  - Drills
  - Desk top or walk through
  - Simulations or critical activity exercises
  - Full BCP

bsi.

Exercise Considerations:
- Resource availability or utilization
- Frequency
- Scope of exercises
- Involvement of suppliers or outsources
- Post-exercise activities

bsi.
Thank you for your support

QUESTIONS