Introduction to Business Continuity Management
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 sites threats</td>
</tr>
<tr>
<td>Determining Choices</td>
<td>Using the Risk Assessment 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 (BCP’s) 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>

* based on ISO 22301 & aligned with other BU’s
What is Business Continuity Management?

The **uninterrupted availability** of resources necessary to run your operation at a level **acceptable** to 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.

Source: BSI; ISO 22301:2012

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.
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

Employer of Choice

A safe and secured workplace environment  
OHSAS 18000 & ISO 22301
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.
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
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>Accidents</th>
<th>Infectious disease outbreak</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aircraft accidents</td>
<td>Kidnap/ ransom</td>
</tr>
<tr>
<td>Airport closure</td>
<td>Landslide</td>
</tr>
<tr>
<td>Robbery</td>
<td>Lawsuit</td>
</tr>
<tr>
<td>Bankruptcy</td>
<td>Layoff</td>
</tr>
<tr>
<td>Berserk employee</td>
<td>Libel/ slander</td>
</tr>
<tr>
<td>Bomb threat</td>
<td>Litigation</td>
</tr>
<tr>
<td>Boycott</td>
<td>Malicious damage</td>
</tr>
<tr>
<td>Business scandal</td>
<td>Murder</td>
</tr>
<tr>
<td>Chemical spill</td>
<td>Negative media exposure</td>
</tr>
<tr>
<td>Civil unrest</td>
<td>Packaging problems</td>
</tr>
<tr>
<td>Class action</td>
<td>Personal threats</td>
</tr>
<tr>
<td>Collapse of structures</td>
<td>Product contamination</td>
</tr>
<tr>
<td>Computer/ IT failure</td>
<td>Professional liability</td>
</tr>
<tr>
<td>Denial of entry</td>
<td>Regulatory changes</td>
</tr>
<tr>
<td>Death (employee or customer)</td>
<td>Rumour and innuendo</td>
</tr>
<tr>
<td>Drug abuse</td>
<td>Sabotage</td>
</tr>
<tr>
<td>Earthquake</td>
<td>Sexual harassment</td>
</tr>
<tr>
<td>Executive succession/ departure</td>
<td>Storm</td>
</tr>
<tr>
<td>Explosion</td>
<td>Suicide</td>
</tr>
<tr>
<td>Extortion</td>
<td>Terrorism</td>
</tr>
<tr>
<td>Fire</td>
<td>Theft</td>
</tr>
<tr>
<td>Flood</td>
<td></td>
</tr>
<tr>
<td>Harbour/ port blockage</td>
<td></td>
</tr>
<tr>
<td>Hijacking</td>
<td></td>
</tr>
</tbody>
</table>
5 (Critical): Very likely the risk will occur
4 (Serious): Likely the risk will occur
3 (Moderate): Occasionally the risk will occur
2 (Minor): Unlikely the risk will occur
1 (Negligible): Very unlikely the risk will occur
The BCMS

PLAN

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

DO

BIA
• Risk assessment
• Treatments

BC Strategy
• Priorities
• Resources
• Protection and mitigation

BC Procedures
• Incident response structure
• Warning and communications
• BC plan
• Recovery

Exercising and testing
• Aims and objectives
• Minimize risk
• Report and action

CHECK

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

ACT

Actions to address nonconformities, Continual improvement
Business Continuity Management System and PDCA

Continual Improvement of BCMS

Interested parties

Establish (PLAN)

Implement & Operate (DO)

Monitor & review (CHECK)

Maintain & Improve (ACT)

Requirements for BC

Managed BC

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

BCM Policy
1. Announced globally on January 24th, 2013

Provision of Resource
2. CT & Station has appointed a BCM nominee with appropriate seniority to be accountable for implementing BCM

IMT
3. Station has formed a Incident Management Team (IMT) with deputies for all key functions

Business Analysis
4. Station has identified activities (operations) that support its key products and services and its priorities for recovery of critical activities

BIA Risk Assessment
5. Station has completed a business impact analysis and has identified and documented the site’s threats

Determining Choices
6. Using the Risk Assessment document the station has, for each of its critical activities identified, available risk solutions

Determining BCP Strategy
7. Station has determined how it will recover each critical activity within its recovery time objective (RTO), including the resources required for resumption

BCP’s
8. Station to create Business Continuity Plans (BCP’s) 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

Maintaining and Reviewing
9. Station has ensured that its BCP arrangements are reviewed and documented at planned intervals

Testing and Exercising
10. 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

* based on ISO 22301 & aligned with other BU’s
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, terroristic 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.
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
BCMS Documentation

TYPICAL HIERARCHY

Level 1
Policy

Level 2
Procedures

Level 3
Documents needed to plan, operate, and control processes

Level 4
Records - evidence of results achieved and activities performed

Overview of the organization and its’ approach to business continuity

High level management documents

Procedures (who, what, why, when, where)

Operational documentation (how)

Records

Copyright © 2012 BSI. All rights reserved.
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
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
Operate & Assess the System

Process Planning “Turtle Diagram”

- **With what?** Resources
- **With Who?** Personnel
- **Inputs** From whom/where
- **Outputs** To whom/where
- **How done?** Methods/Documentation
- **What results?** Performance indicators

Process (specific value added activities)
Resumption of Activities

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

bsi.
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 HR activities may not be equally suitable for IT or H&S)
- 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
### 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?
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
Testing & Exercising

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
Testing & Exercising

BCM Exercising

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