

\*connectedthinking

# Business Continuity Planning Professional Development Workshop

December 11, 2006

Presented by **Bruce L Scott** FCA, FCCA, CISA, MBA, ABCP, CISM

Partner, Business Continuity & Risk Services, PricewaterhouseCoopers

[bruce.scott@jm.pwc.com](mailto:bruce.scott@jm.pwc.com)

876-932-8335



# Presentation Outline

- What is business resilience/continuity planning?
- Why is business continuity planning important?
- How should CDERA influence companies, entities, to respond to the business continuity risk challenge?
- Is your company prepared for a major disaster?
- The business continuity planning cycle
- PwC's proprietary methodology and project execution approach
- Demonstration of business resumption plans & IT disaster plans
  - Bank Limited
- Keys to successful business continuity planning
- Twelve things to consider after this workshop
- Typical BCP project steps
- Other BCP issues to consider
- Closing remarks

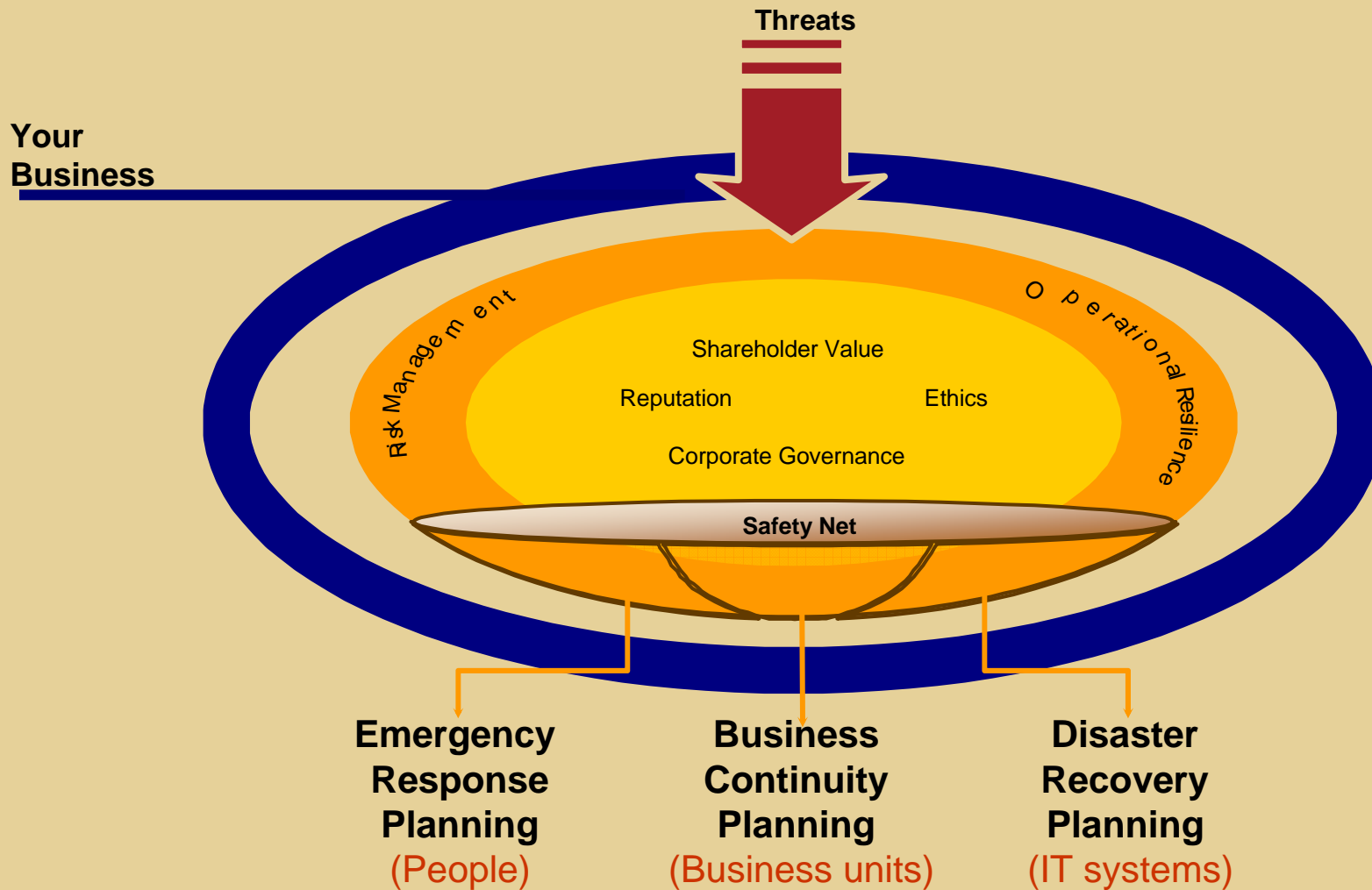
# What is Business Continuity Planning?



A definition:

*Procedures that are instituted to continue the operations of your business despite a significant interruption (to its buildings, IT systems or employees) with the ultimate objective of restoring the business to pre-disaster levels.*

# What is Business Continuity Planning?



# What is CDERA's role in sensitising large corporations in member states?

*How can CDERA influence its member states recovery efforts at the business and government services level, through its Board and Council bearing in mind the following:*

- 1. Important government services should be restored as soon as possible after a disaster*
- 2. Large corporations that employ a large number of the population should know what to do to continue their businesses despite any type of disaster (hurricane, fire, earthquake etc)*
- 3. How can CDERA sensitise and influence these important institutions in each of its member countries to ensure that businesses recover as soon as possible after a disaster?*

# Why is Business Continuity Planning Important?

- Protection of people (most important)
  - Protection of the life and safety of employees and customers
    - The people cost was the highest cost in 9/11
- To stay in business
  - Possible permanent closure of companies in the Financial Services Division could be the result of a disaster. *A 2003 study of a local bank similar to First Global Bank revealed that permanent closure could result in 3-5 days where there is a disaster and there is no recovery of the business in this period of time (3 to 5 days)*
  - You may survive a disaster without a plan, but researchers confirmed that....
    - Generally, 93% of these companies go out of business **within 5 years**

# Why is Business Continuity Planning Important?

- Maintenance of your brand and reputation
- Stakeholder expectations
  - regulators (BOJ BCP BEST PRACTICE TO BE ISSUED SOON)
  - international business partners
  - investors/shareholders (Barbados, Trinidad and Jamaica Stock Exchanges)
- Competitive advantage
  - Your competitors have started to move in this direction
    - Imagine a disaster in your area and your competitors got back up and you didn't
  - Hurricane Ivan

# Why is Business Continuity Planning Important?

- **Because disasters do happen!**
  - Fire damage is perhaps the biggest threat
    1. Electrical problems
    2. Arson

# Why is Business Continuity Planning Important?

- **Because disasters do happen!**

## **Recent local newspaper report:**

**Shopping centre fire leaves millions of dollars in damage**  
Observer Reporter, Tuesday, September 02, 2003

**FIRE** yesterday caused **millions of dollars in damage to several businesses** located on the first floor of the Villa Shopping Centre on Main Street in Mandeville, renewing calls by residents for adequate water supply in the parish.

Cause of fire; unknown up to press time

# Why is Business Continuity Planning Important?

- **Because disasters do happen!**

## **Recent local newspaper report:**

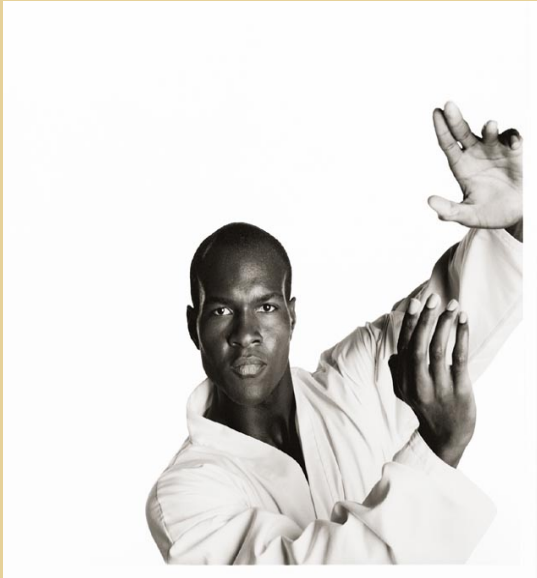
### **\$20m Plaza Fire – The Jamaica Gleaner (Aug 2000)**

*Large clouds of **smoke rise from the Sports Gallery store in the Springs Plaza, St. Andrew** yesterday as firefighters battle the flames. Firefighters and the owner of the store, which was not insured, estimated the damage at **\$20 million**.*



Cause of fire: Electrical problems

# How should companies respond to the business continuity risk challenge?



*How should companies prepare and respond to real threats such as fires, and other disasters?*

# How should important government services and other companies in member states respond to the business continuity risk challenge?

- Recent Gartner survey findings on how American companies have responded:
  - 85% of large companies (USA) have IT recovery plans
  - Only 25% of these companies have business unit recovery plans (e.g. for treasury, equity trading, accounts etc)

Note:

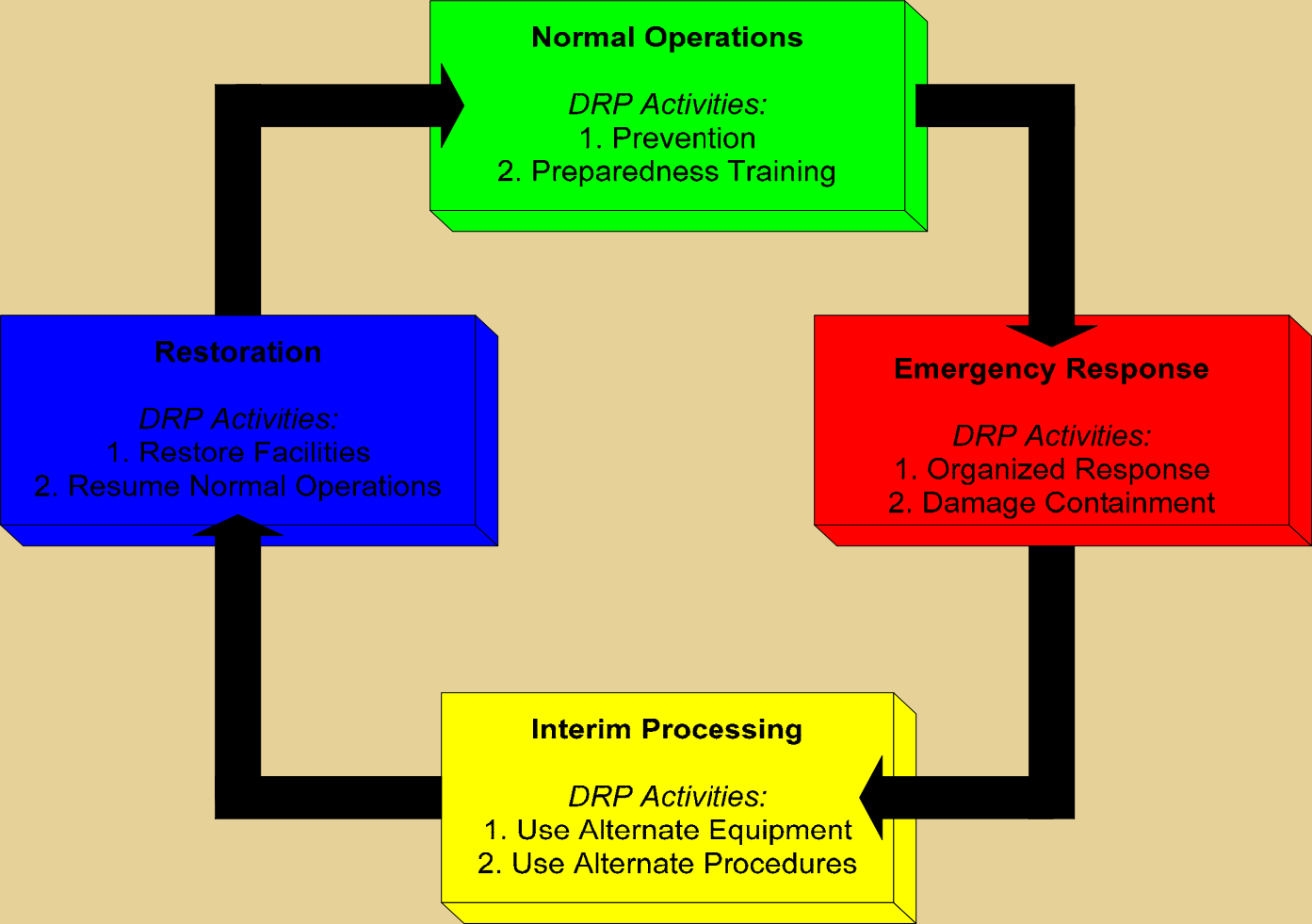
A growing number of Caribbean companies are making efforts but plans tend to be IT centric and ignore the business units **(this is not adequate for an effective recovery – 9/11 confirmed this!)**

# Are Caribbean Government entities, financial Services Companies & Other Companies prepared for a major disaster?



*What if you were a CEO of a major Caribbean bank and got a call tomorrow morning at 7:00 a.m., saying that a fire destroyed all of the head office building, would you know what to do in the next minute after receiving the call?*

# Business Continuity Planning Life Cycle



# Our proprietary methodology and project execution approach

**PwC's proprietary methodology in developing business unit & IT disaster plans.**  
(methodology also covers the 4 stages in responding to a disaster)



# Risk Assessment: IT (Computer Room)

**Objective:** Identify threats that could lead to disasters

**Threats are:**

1. Fire protection re the computer room
2. Electrical power in the computer room
3. History of problems in the computer room
4. Environmental controls & systems in computer room
5. Entry protection to computer room
6. Physical protection of computer equipment
7. Data tape management
8. Single points of failures & redundancies
9. Insurance coverage
10. Information security

# Risk Assessment: Business Units (Building)

**Objective:** Identify threats that could lead to disasters

**Threats are:**

1. Fire protection (building in general)
2. Electrical power (building in general)
3. History of problems of the location of the building
4. Environmental controls (building in general)
5. Entry protection of persons accessing the building
6. Physical protection of utilities room (e.g. telephone, etc)
7. Insurance coverage

# Risk Assessment: IT & Business Units

## How to conduct a risk assessment?

1. Complete computer room questionnaire
2. Complete building questionnaire
3. Interview the following persons:
  - a) Building/property manager
  - b) Administration or Office Manager
4. Facilitated workshop with key business department heads  
(review of likelihood and impact of threats)

# Risk Assessment: IT & Business Units

## How to report findings:

1. Identify areas that are deficient (fire, single points of failures etc)
2. Estimate cost of addressing deficiencies
3. Submit cost for approval to Board & Senior Management
4. Risk accept & monitor those deficiencies that are not cost effective to fix
5. Rank threats according to High, Medium or Low risk or use some other measure (SHOW GRAPHICAL EXAMPLES & SAMPLE REPORT)

# Business Impact Analysis (BIA): IT

**The following information is obtained during the BIA for each business unit (e.g. accounting, marketing etc) concerning IT :**

1. The tangible & intangible impact of an IT disaster
2. Specific systems & applications used
3. IT downtime tolerance i.e. how long units could survive without IT
4. The existence of manual alternatives/workaround procedures

# Business Impact Analysis (BIA): IT

## Usage of the BIA information:

1. To make the business case for spending on IT disaster planning
2. To identify the recovery order of the IT systems
3. To identify the most efficient IT recovery strategy based on the downtime tolerances of the business units & the impact of a disaster (e.g. hot site, warm site, cold site, do nothing, etc)
4. To identify the business units that are most dependent on IT systems

# Business Impact Analysis (BIA): Business Units

**The following information is obtained during the BIA for each business unit (e.g. accounting, equity trading etc):**

1. The same information re loss of IT systems (see previous slides)
2. But, the following additional information is needed
  - a) Identification of all business functions performed in each dept
  - b) Classification of business functions in order of criticality
  - c) Identification of vital records required by the functions
  - d) Identification of internal & external dependencies
  - e) Identification of inputs/outputs required for each business function

# Business Impact Analysis (BIA): Business Units

## Usage of the BIA information:

1. To make the business case for doing the business unit plans
2. To identify the minimum number of business units that must be recovered in order to stay in business (e.g. 5/10)
3. To identify the critical business processes that must be available to continue the business at an acceptable level
4. To identify the most efficient recovery strategy based on the downtime tolerances of the business units, the impact of a disaster & the minimum resource requirements (e.g. hot site, warm site, cold site, etc)

# Strategy Selection: IT

After identifying the most critical *IT systems*, a strategy or a menu of strategies should be developed to protect these resources:

1. **Do nothing** – risk may be acceptable or there could be enough time to respond without a formal plan (e.g. RTO of 4 hrs v 40 days)
2. **Insurance** – provides financial recompense (brand not protected)
3. **Loss mitigation** – i.e. implementing redundancies etc
4. **Develop a business continuity plan** – this is an approach to continuing the business despite a significant disruption. *This will be influenced by the RTOs of the IT systems – FUNDAMENTAL!*

# Strategy Selection: Business Units

After identifying the most critical *business units*, a strategy or a menu of strategies should be developed to protect the business units:

1. **Do nothing** – risk may be acceptable or there would be enough time to respond without a formal plan (e.g. RTO of 4 hrs v 40 days)
2. **Insurance** – provides financial recompense (brand not protected)
3. **Loss mitigation** – i.e. implementing redundancies etc
4. **Develop a business continuity plan** – an approach to continuing the business despite a significant disruption. *This will be heavily influenced by the RTOs of the business units – FUNDAMENTAL!*

# Strategy Selection: IT & Business Units

The selected strategy will be influenced by the following

1. Minimum resource requirements:
  - a) **PCs**
  - b) **People**
  - c) **Vital records**
2. Internal & external dependencies (fire vs hurricane?)
  - a) **Suppliers**
  - b) **Customers**
3. Recovery Time Objectives
4. Impact: Financial, Reputational, Operational & Legal

# Strategy Selection: IT & Business Units Summary

The selected strategy will be influenced by the following

1. Do nothing
2. Replicate everything
3. Choose a point between point 1. and 2. above
4. Also must make plan assumptions
  - Key persons are alive
  - Data will be available
  - No access to the building that is affected i.e. all record, equipment, resources on the building are not accessible
  - Disaster lasts for up to 5 days

# Strategy Selection: IT & Business Units Summary

The selected strategy will be influenced by the following

1. Do a short list of the possible recovery options
2. Highlight the advantages and disadvantages of each
3. Estimate the cost (one time and recurring for each)
4. Make recommendation to the Board

# Simulation/Plan Development

1. Having selected a recovery strategy the plan can now be developed
2. The actual plan will provide guidance on the 4 stages in responding to a disaster (see next slide)

OR

1. Simulation of a real disaster can be done before the plans are written
  - a) Identification of a realistic scenario
  - b) Development of a script (similar to a play or movie)
  - c) Execution of the simulation, facilitated by PwC
  - d) Requires all senior managers of Bank Limited
  - e) This is a powerful exercise with immediate results!
  - f) Simulation session – lasts to 3 hours
  - g) Debrief & lessons learned session – 1 1/2 hours

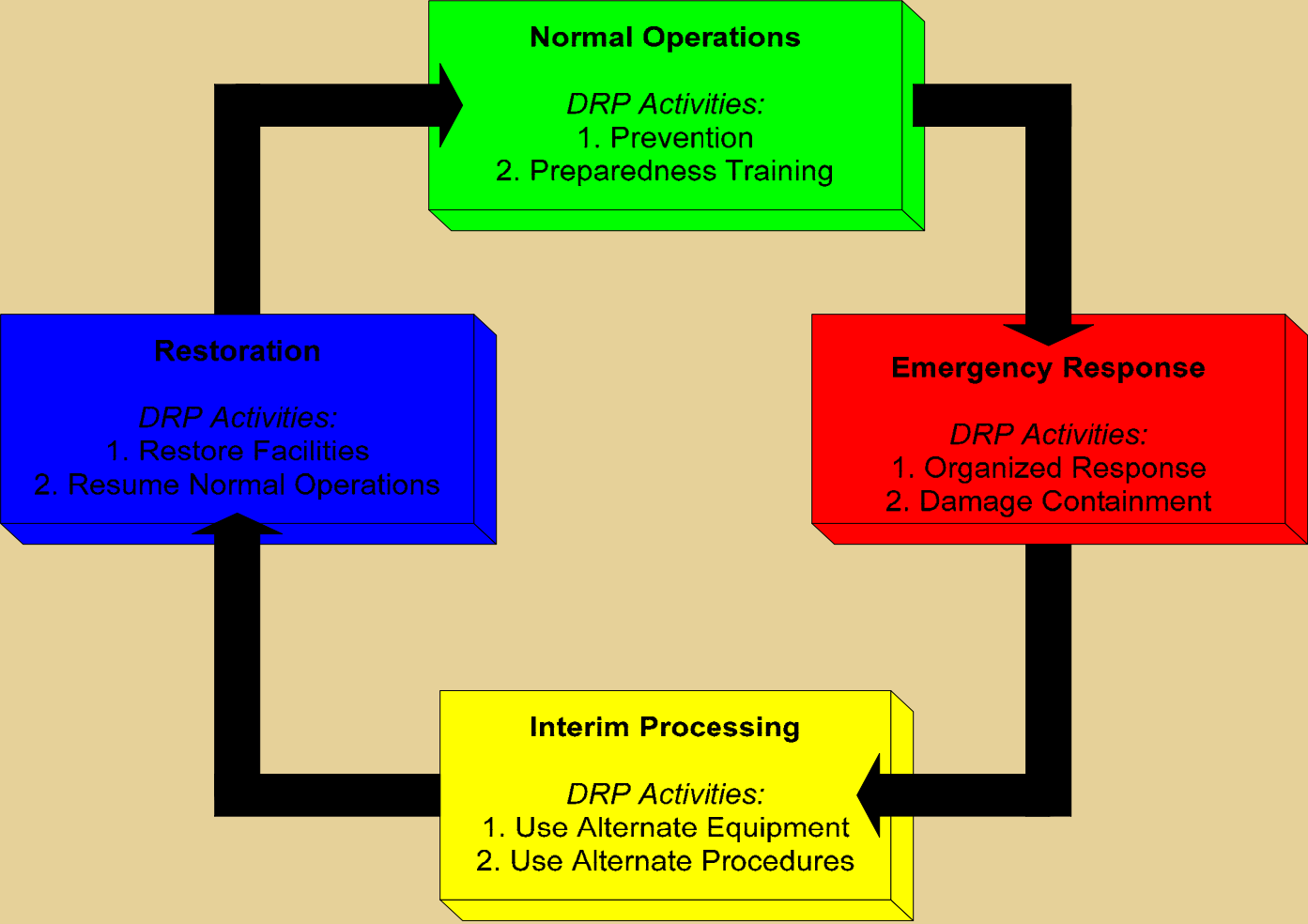
# Implementation

1. Training and awareness
  1. Recovery teams
  2. Members of staff
  3. Executives and Board members
  
2. BCP Organisation
  1. BCP Committee
  2. BCP Coordinator
  3. BCP Champions
  4. Leveraging aspects of a company's natural structure
  
3. Plan Maintenance
  1. Annual updates
  2. Method
  3. Company changes

# Implementation

4. Testing: simulations, call test and walkthroughs
5. BCP Prerequisites: Vital records management, system backups
6. BCP Budget

# Business Continuity Planning Life Cycle



# BUSINESS RESUMPTION PLAN – BANK LTD

## TABLE OF CONTENTS

### Part 1

- I. Plan overview (objectives, assumptions, scope, team responsibilities, recovery strategy)
- II. Restoration, Testing & Maintenance Procedures

### Part 2

- I. Initial response – during normal business hours (6 recovery teams coordinate this response)
- II. Initial response – after normal business hours
- III. Settle at the alternate site, restore vital records and perform short term work arounds
- IV. Invoke degraded mode:
  - 1. Asset & Portfolio Mgt (6 critical functions) – RTO 8 hrs
  - 2. Equity Trading – (4 critical functions) – RTO 8hrs
  - 3. Mutual Funds (4 critical functions) – RTO 8 hrs
  - 4. Pension Management & Administration (4 critical functions) – RTO 8 hrs
  - 5. Administration (2 critical functions) – RTO 8 hrs
  - 6. Finance & Accs (3 critical functions) – RTO 8 hrs

### Appendices

- 1. Contact Listing – Recovery Teams
- 2. Contact Listing – Internal & External
- 3. Vital Records Required
- 4. Minimum Resources Required
- 5. Team roles and responsibilities (team members of the business units)

*For Illustrative Purposes Only*

**This document is proprietary to PricewaterhouseCoopers and cannot be reproduced / copied without permission.**

# IT DISASTER RECOVERY PLAN – BANK LTD

## TABLE OF CONTENTS

### Part 1

- I. Plan overview (objectives, assumptions, scope, team responsibilities, recovery strategy)
- II. Restoration, Testing & Maintenance Procedures

### Part 2

#### Emergency Response

- I. Initial response – during normal business hours
- II. Initial response – after normal business hours

#### Recovery Activities

- I. Disaster Recovery Coordinator – Tasks & Activities
- II. IS Emergency Management Team – Members, Tasks & Activities
- III. Network Team – Members, Tasks & Activities
- IV. Operations Team – Members, Tasks & Activities
- V. Application Team – Members, Tasks & Activities
- VI. Administrative Support Team – Members, Tasks & Activities

#### Appendices

- I Recovery Time Objectives for Critical IT Applications (Banking App – 8hrs, CRM – 8hrs, GL – 8hrs)
- I. Key Employee Listing
- II. Critical Inventory Listing
- III. Key Vendor Listing
- IV. Vital Records

*For Illustrative Purposes Only*

**This document is proprietary to PricewaterhouseCoopers and cannot be reproduced / copied without permission.**

# Keys to Business Continuity Planning success

*The tragic events of September 11 indicate that those companies that had documented and tested Business Continuity plans were able to resume critical business operations in a matter of hours. Companies that recovered found the following to be true:*

- Critical elements of BCP include:
  - Board and senior management commitment (financial & otherwise)
  - Focus on critical business processes in the business units (i.e., not just IT)
  - BCP steering committee and BCP coordinator
  - Understanding the total cost of a business continuity program
  - Ownership of the business unit plans by the business unit managers

# Twelve Things to Consider After You Leave This Workshop

1. Solicit strong board level support and commitment to business continuity.
2. Appoint a Business Continuity Planning Coordinator /Owner
3. Perform a facilities & IT risk assessment along with a business impact analysis
4. Use a scenario-based planning approach, which is based on a “worst case” model.

# Twelve Things to Consider After You Leave This Workshop

6. Recognise the importance of having off-site storage and recovery locations operations located at a safe distance.
7. Develop established procedures for the electronic storage of vital records.
8. You should ensure that you have a robust technical recovery strategy and aggressive manual work arounds while you wait for the recovery of your IT systems.

# Twelve Things to Consider After You Leave This Workshop

9. Ensure that a system of frequent and extensive testing of your business continuity plans are in place to keep your plans current.
10. Ensure that a strong plan maintenance process is in place to keep your plans current.

# Twelve Things to Consider After You Leave This Workshop

11. Understand clearly what your insurance company will and will not cover.
12. Ensure that the plan has clear emergency response procedures and an Emergency Management Team that is empowered to declare a disaster

# Typical Steps in a BCP Project: Objectives & Scope

Clearly State the Project Objectives:

- To deliver business continuity (including IT disaster recovery plans) for the departments within your company

Identify the Project Scope:

- Locations used by your company to conduct business
- What are the addresses for these locations?

# Typical Steps in a BCP Project: Establish the Project Time Line

- Kick off meeting
- Interview of Building & IT Manager – IT & Facilities Risk Assessment
- Interviews of Department Managers – Business Impact Analysis (average interview is 60 to 90 mins)
- BIA & Facilities Risk Assessment Reports
- Development of Simulation Scenario with the Project Coordinator
- Simulation Testing - (2 meeting rooms at a Hotel) – 60 minutes
- Simulation Debrief & Strategy Selection (45 minutes)
- Plan Development
- Final Plans and Close Out Presentation

# Typical Steps in a BCP Project: Confirm Project Structure, Time and Cost

- Business Continuity Steering Committee
  1. Local - Department heads at Bank Limited
  2. Coordinator - BCP
- Project Sponsors
- Project Coordinator
- Project Team
- Average time to complete plan varies ... but ranges from 1 month to 6 months (depends on the complexity of the company)
- Average Cost also varies US\$15K to US\$250K

# Other BCP Issues to Consider

1. Will my insurance company recognise my BCP effort?
2. Do you need a full time BCP employee?
3. Why can't I just take a template off the internet and simply populate it?
4. Why bother to do plans when, we have never had a disaster before?

# Other BCP Issues to Consider

5. What are the one time cost and the recurring cost of a BCP program?
6. What is the profile of the BCP Owner and position in the organisation?
7. What is the difference in approach in plan preparation between preparing for a natural disaster such as hurricane and a localise disaster such as a fire
8. What are the steps that are taken, immediately after a disaster, right up to the point of restoration to pre-disaster levels?

# Quiz

## True or False Questions

Be prepared to defend you answers!

# Simulation Testing: Preview

If time allows, show and demonstrate from a previously edited script how the simulation process works

# Presenter Profile

**Bruce Scott, FCA, FCCA, CISA, MBA, ABCP, CISM**

**Bruce is the partner in charge of our Business Continuity/Resilience Practice in Jamaica. He has been involved in operational and systems risk management since 1993. Bruce has attended overseas courses in Business Continuity Planning (BCP) and has consulted on the business continuity plans for several Caribbean and Canadian companies. Bruce spent six months in the Business Continuity/Resilience practice of our GRMS service line in the PricewaterhouseCoopers office in Toronto, Canada. While in Toronto, Bruce worked on large business continuity planning engagements for companies such as AstraZeneca, Sears Canada and an internal business continuity project for PricewaterhouseCoopers Canada. He has completed the development of the entire business continuity program for several leading Caribbean banks and companies in other industries. He is a certified BCP consultant, with the designation Associate Business Continuity Planner (ABCP) with the Disaster Recovery Institute International, which is based in the USA. He is also a chartered accountant (FCA), a Certified Information Systems Auditor (CISA), a Certified Information Security Manager (CISM) and holds an MBA degree from Manchester Business School.**

