



# Business Continuity

---

## CGBS/CARTAC IT Workshop for Regional Bank Examiners

June 23 – 25, 2009  
Georgetown, Guyana

David A. Wong  
Senior Systems and Technology Officer  
Financial Institutions Supervisory Division  
Methods, Analysis and Quality Review Department  
Bank of Jamaica  
[www.boj.org.jm](http://www.boj.org.jm)



# Agenda

---

- Misconceptions
- BCP vs. DRP
- The BCP process
- Recovery Alternatives
- BCP Testing
- Examiner Expectations and Challenges

## Misconception

---

- BCP and DRP are the same and focus on IT
  - terms used interchangeably, but are different
  - prior to major catastrophes only DR was important
  - after major catastrophes we realized that operations was also important (not just restoring IT)

## What is Business Continuity Planning? (BCP)

---

The process to ensure the maintenance or recovery of operations, including services to customers when confronted with adverse events such as:

- Natural Disasters
- Technological Failures
- Human Error
- Terrorism



## What is Disaster Recovery Planning? (DRP)

---

- covers data, hardware and software critical for a business to restart operations in the event of a natural or human-caused disaster.
- Includes plans for coping with the unexpected or sudden loss of key personnel.



## BCP Facts

---

- o BCP is a business focus, not just IT – a plan to continue business
- o Includes a DRP and IT
- o Enterprise-wide
- o Board and Senior Management responsibility
- o Even if outsourced, still must implement BCP addressing in-house processes and equipment



## Grand Cayman and Hurricane Ivan

---

- In 2004 Grand Cayman was decimated by Hurricane Ivan
- Total impact more than the combined 2004 season damage to Grenada, Jamaica, Dominican Republic and Bahamas
- Damage included the destruction of the Island's primary telecommunications landing station

**A BCP is critical!!**



## The BCP Process

---

- Must be enterprise-wide
- Must include critical functions/processes
- Must begin with Business Impact Analysis (BIA)
- Must include:
  - Risk Assessment
  - Risk Management
  - Risk Monitoring (incl. testing)

## Business Impact Analysis

---

- Should cover critical processes and functions (not just IT)
- Identify risk : impact of uncontrolled non-specific events  
(what and how much is at risk)
- Estimate maximum allowable downtime
- Recovery point objectives
- Recovery priorities – essential personnel, technologies, facilities,  
communication, vital records and data
- Legal and regulatory requirements

## What do banks consider in their BIA

---

- Mission critical functions and personnel
- Specialized equipment
- Single points of failure - Eg. Internet access for certain depts.
- Outsourced relationships
- Minimum # of staff
- Specialized forms, communication devices, necessary supplies
- Security controls
- Emotional support and family care

## The Risk Assessment

---

- **Develop realistic threat scenarios** : stress test based on assumptions against BIA
- **Consider probability of an occurrence**
- **Impact analysis** : impact of each occurrence in threat scenarios
- **Gap analysis** : comparison of what kind of plans to maintain

## Threats / Events / Disasters

---

- Disruption to operation of critical processes
- Adversely impact business operations

Types:

- Natural
- Human
- Environmental
- Technical
- Expected services no longer supplied



## Risk Management

---

“The deeper the understanding of risk is the better the response to disaster or difficulty, and the stronger and more resilient one is”



## Risk Management

---

- Focuses on maintaining, resuming and recovering critical business processes
- Documented strategies and procedures
- Identify individual and team responsibilities
- Flexible
  - internal and external conditions, as well as threat scenarios change
- Consider all interdependencies
  - Eg. communications

## Choosing the Recovery Strategy

---

- Selection based on:
  - BIA
  - Criticality of functions/systems
  
- Key Metrics:
  - Recovery Point Objective (RPO)
  - Recovery Time Objective (RTO)

## Recovery Point Objective (RPO)

---

“A measure of how much data can be lost when a disaster occurs.”

Typically, this is the difference in time between when the disaster happens and when the last back-up occurred.

## Recovery Time Objective (RTO)

---

“A measurement of how long the business can survive without the systems being in place to run the specific business processes”

Important factors:

- Ensure worst case scenario is planned for
- Consider the amount of time required to catch-up

## Note!

---

The RTO and RPO will significantly determine the BCP/DR cost.

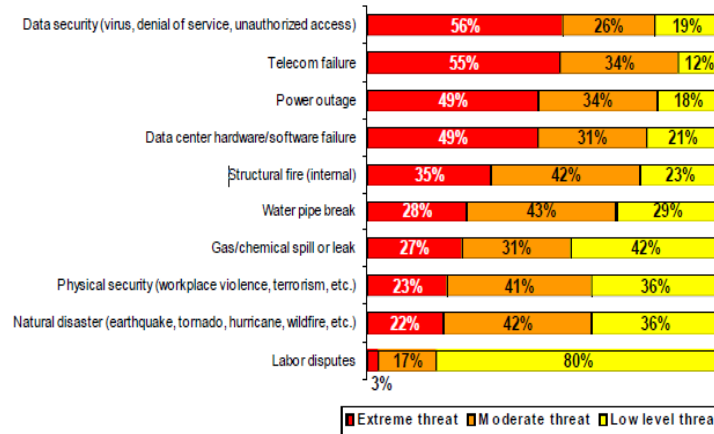


dilbert bcp budget video.mp4

## Classification of Systems

Typically 4 classification levels:

- Critical
  - Must be replaced by identical system
  - Cannot use manual methods
  - Have a very low tolerance to interruption
  
- Vital
  - Can be performed manually for a limited time
  - Have lower cost of interruptions
  
- Sensitive Systems
  - Can be performed manually for extended time
  
- Non-Critical Systems
  - Have little or no cost from interruptions



Listed above are types of events that may pose a threat to business continuity at your organization. Using a 10-point scale, where '10' means that the event poses a 'extreme threat' and '1' means that the event 'does not pose a threat,' please rate the events on the level of threat each poses.

Source: Iron Mountain white paper  
 "The business case for disaster recovery planning : calculating the cost of downtime"

## Recovery Alternatives

---

There exists:

- Hot Sites
- Warm Sites
- Cold Sites
- Reciprocal Agreements
- Duplicate Information processing facilities

"Every recovery effort is different and recovery time is really dependent on the complexity of the system, amount of data to be restored, method, etc.

Therefore, the following recovery times are generalizations"

## Recovery Alternatives

---

### Hot Sites [immediate to 4 hours to recover]

These facilities are:

- Fully configured and ready to operate
- Available within hours
- Must be fully compatible
- Only staff, programs, data and documentation required

Disadvantages:

- Costs may include subscriptions, monthly fees and activation
- Costs are usually high (can be covered by insurance)
- For short term use (typically because of cost)

## Recovery Alternatives

---

### Warm Sites [hours or days to recover]

These facilities are:

- Partially configured (eg. Cabling, A/C, Backup Power Supply)
- Network connections and selected peripheral equipment (servers)
- Lower cost than hot site

### Cold Sites [days to weeks to recover]

These facilities:

- Have very basic facilities (eg. Cabling, A/C, but no actual hardware)
- Are the lowest cost option

*\*Not usually practical for most institutions and not recommended for modern IT environments*

## Recovery Alternatives

---

### Reciprocal Agreements

- Made between two or more institutions with similar facilities
- They provide processing time to each other in an emergency
- Entities not in close proximity and so not susceptible to same occurrences

These agreements:

- Must be written
- Must include necessary activities

## Recovery Alternatives

---

### Duplicate Information Processing Facility (Mirroring)

These facilities are:

- Dedicated self-recovery site
- Allows mirroring of data that is primarily being processed at a different site

## BCP/DR Training and Communicating

---

- Key Employees
  - they should be directly involved in development and training
- Plan to be communicated to all employees
- Customers should be aware
  - Eg. How to contact the bank or what to do in event of disaster
- Training should be regularly scheduled and updated
  - (cross-training in event that key individuals not available)

## BCP/DR Training and Communicating

---

- Alternate communication channels should be identified
- Key persons who are authorized to initiate the plan should be designated
- Lists of emergency contacts
  - (telephone numbers, email addresses, physical addresses, vendors, regulatory agencies, emergency services)

## Testing

---

- Mock Drills - should be performed periodically (eg. Fire drills or role playing)
- Unmanned - sending the back-up to a recovery site to be loaded and run
- Functional - includes actual moving personnel to another site
  - Usually done on varying levels, as opposed to doing a full scale test
- Full scale - comprehensive and includes all aspects of the plan

## Testing Imperatives

---

### Tests should :

- be done at least annually (full scale)
- Include backup and offsite material
- Include reports and analysis (including follow-up)
- Include independent review (eg. Internal Audit)

## Examiner Expectations

---

- Ensure written, comprehensive BCP and DRP
- Look for: BIA, Risk Assessment (threat scenarios), strategies and procedures that are in place
- Look at communication to employees (how often?)
- Look at the training (who conducted it, frequency, what is included)
- Look at BCP tests (type, how often, results, review the reports)

## Common Examination Deficiencies

---

- No BIA
- Plans not sufficient – too focused only on IT
- Incomplete risk assessment
- Inadequate testing
- Pandemic not addressed
- WORM BCPs and DRPs

## Questions

---



**David A. Wong**  
Senior Systems and Technology Officer  
FISD/MAQR  
Bank of Jamaica

CGBS/CARTAC Regional IT WORKSHOP

## Resources

---

- Slide Show adapted from a presentation by Susan Orr from Susan Orr Consulting
- FFIEC Influenza Pandemic Preparedness
- FFIEC IT Security Handbook
- FFIEC IT Operations Handbook
- FFIEC IT Business Continuity Planning Handbook
- Basel Committee on Banking Supervision: The Joint Forum – High Level Principles for Business Continuity

## Resources

---

### **White Papers:**

- Business Continuity Planning: Ensuring 'Business as Usual' When the Unusual Happens by: Paul Fochler
- The Business Case for Disaster Recovery Planning: Calculating the Cost of Downtime by: Iron Mountain
- Be Prepared – Crafting and implementing a Disaster Recovery Plan by: James Swann
- A Supervisory Perspective on Disaster Recovery and Business Continuity by: Roger W Ferguson Jr (Board of Governors of the US Federal Reserve System)
- Ten Ways to Protect your IT Infrastructure by: Carl Walker

## Resources

---

### **Case Study:**

- One Year on From Hurricane Ivan: What Lessons have been Learnt?  
By: Torrin Stafford