A business case for establishing Business Continuity Plan (BCP)
Contents

1. What is Business Continuity?
2. Business Benefits
3. Implementation Roadmap
What is Business Continuity?

A business case for establishing a Business Continuity Plan
9/11 for Pakistan
Happened in Karachi (June 26, 09)
Suicide Attack in Lahore (May 27, 09)
Thanks to KESC
Berger Paints
Fire at Shahra-e-Faisal Building
The Reality of Business Continuity

- 43% of US companies never reopen after a disaster and 29% more close within 3 years.

- 20% of small to medium size businesses suffer a major disaster every 5 years.

- 78% of organizations which lacked contingency plans but suffered catastrophic loss were gone within 2 years...most had insurance, and many had business interruption coverage!

Is This An Effective Management Strategy In the Face of the KNOWN Risks!

YES!

NO!
The impact on shareholder value

What is Business Continuity Management?

Business Continuity Management (BCM) is a holistic management process that:

- Identifies potential impacts that threaten an organization,
- Provides a framework for building resilience and the capability for an effective response,
- Safeguards the interests of key stakeholders, reputation, brand and value creating activities.
Success or Failure?

Time

Level of business

A

Fully tested effective BCM

B

No BCM – lucky escape

C

No BCM – usual outcome

Critical recovery point
Business Benefits

A business case for establishing a Business Continuity Plan
Key Benefits (1)

- **To Business**
  - Gain reputation as “Safe and Secure Organization”
  - First mover advantage
  - Cost effectiveness = Higher profitability
  - Better compliance with laws and regulations
  - Better continuity in case of any disaster

- **To Operations**
  - Better risk management & risk reduction
  - Better cost control
  - Defined SOPs

- **To IT**
  - Identification and control of information assets
  - Better risk management
  - Defined SOPs
  - IT Disaster management
Key Benefits (2)

- Better policies, procedures and working templates
  - Business continuity
  - Information security
  - Related roles and responsibilities
  - Organization wide awareness
  - SAP related and general IT infrastructure
  - Use of network services
  - Mobile computing
Key Benefits (3)

- Identification of Business Critical processes
  - Process identification
  - Process ranking according to business criticality
  - Continuity strategies for critical processes

- Business Continuity planning
  - Business Impact Analysis (BIA)
  - BCP for all areas under scope
  - BCP awareness, testing and exercises
Key Benefits (4)

- Information Asset Management
  - Information Classification
  - Information Asset Identification & Classification
  - Employee Skill Management

- Risk Management
  - Identification and Analysis of Risks
  - Treatment of Risks
  - Development of Risk Management Approach & Criteria
Key Benefits (5)

- Better Description of Roles & Responsibilities
  - Job description related to information security
  - Pre-hiring controls
  - During employment personnel development
  - Post-employment controls

- Physical Security
  - Identification of Secure Areas
  - Equipment Security
Key Benefits (6)

- **Communications & Operations Management**
  - Documented SOPs
  - Segregation of duties
  - Third party service delivery management
  - System planning & acceptance
  - Data backup and recovery
  - Network security
  - Media handling
  - e-Commerce

- **Access Control**
  - Access control policy and procedures
  - User, network and OS access control
  - Application and mobile access control
Key Benefits (7)

- Regulatory compliance
  - All applicable laws
  - Intellectual property rights

- Framework for Continual Improvement
  - Regular Internal Audits
  - Corrective & preventive actions
Implementation Roadmap

A business case for establishing a Business Continuity Plan
Implementation Roadmap

Phase 1: **Scoping & Planning**

Phase 2: **Understanding the Organization**

Phase 3: **Risk Assessment and Control**

Phase 4: **Implementation of Mitigation Strategies**

Phase 5: **Training for Audit and Internal Audit**
Phase 1: Scoping & Planning

**Awareness**
- Awareness Sessions
- Implementer Trainings

**Team Formation**
- Establishing Management Steering Group
- Establishing working groups

**Project Scoping**
- Identification of geographical scope
- Identification of functional scope
- Documenting and agreeing the scope of the assignment
Phase 2: Understanding the Organization

### Process Identification
- Identification of functions under scope
- Identification of processes under scope

### BIA
- Identification of business impact if process does not work
- Prioritizing processes based on time criticality
- Presenting report to the management

### Asset Registration
- Identification & classification of information assets in the organization
- Asset value assessment
- Asset ownership identification
Phase 3: Risk Assessment and Control

**Risk Assessment**
- Identification of application threats, and risks
- Analyzing probability and impact of risks

**Risk Threshold**
- Calculating risk threshold
- Defining risk acceptance criteria

**Development of SOA**
- Selection of right controls to handle the identified risks
- Implementing risk threshold and acceptance criteria
- Developing and presenting SOA
Phase 4: Implementation of Mitigation Strategies

Security Controls
- Developing processes and procedures for information security controls

Mitigation Planning
- Identifying right mitigation strategies
- Planning for implementation

Business Continuity Plan
- Development of Business Continuity Plan
- Desktop exercise of BCP
Phase 5: Training for Internal Audit and Internal Audit

**Internal Audit Training**
- Hands-on internal audit trainings for selected individuals
- Internal audit trainings on both standards

**Internal Audit**
- Conducting first internal audit
- Developing Internal Audit report

**Audit Findings**
- Detailed assistance in closure of audit findings
- Identification of corrective and preventive actions
Thank You!

contact@businessbeam.com