

BIA

- ❖ *DigitalSherlock.com | SafeHack.com*
- ❖ *Date: 2005/05/27*
- ❖ *Document Name: business_continuity_planning.pdf*
- ❖ *GNU Free Documentation License*
- ❖ *Version 1.00, 2005-05-27*
- ❖ *Copyright © 2005 Adonis, MSc, Eng, CISSP, Security+, CEH, GSec, MCSE, etc.*
- ❖ *Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or any later version published by the Free Software Foundation.*

❖ **Scope and Plan initiation**

- **Help Identifying Business Critical Functions**
- **Top down approach**
- **Responsability**
 - **A statement of organizational responsibility**
 - **All tasks should be divided and assigned to logical individuals**
- **Authority**
 - **A statement of importance**
 - **A statement of priorities**
 - **A statement of urgency and timing**
 - **In times of crisis, It is important to know who is in charge**
 - **Clear-Cut authority aid in reducing confusion**
- **Executive Management**
 - **Executive commitment and support MOST CRITICAL**
 - **Initiates project, gives final approval, gives ongoing support**
- **Senior Functional Management**
 - **Has ultimate responsibility for all phases of the plan**
 - **Senior Management support is critical**
 - **Identifies and prioritizes time critical systems**
 - **Participate in implementation and testing**
 - **Due care**
 - **Doing the RIGHT THING**
 - **Due Diligence**
 - **CONTINUAL EFFORT of making sure right things take place**
- **Central BCP Program Committee**
 - **Responsible to create, implement and test the plan**
 - **Made up of**
 - **Senior Management**
 - **Business Units**
 - **Information Systems**
 - **Security Administrator**
 - **Corporate auditors due to the legal issues**

❖ **Business Impact Analysis (BIA)**

- **Objective**
 - **Help business understand the impact of a disruptive event**
 - **Is a process used to help business units understand the impact of a disruptive event**

- **A vulnerability assessment is often a part of the BIA process**
- **It identifies the company's critical systems needed for survival**
- **Helps to document what impact a disruptive event will have on the business**
- **Risk assessment and analysis needs to be performed to evaluate all potential threats**
- **BIA has three goals:**
 - **Criticality Prioritization-**
 - ♦ Determine critical and necessary business functions
 - ♦ Every critical business unit process must be identified and prioritized
 - ♦ Determine resource dependencies
 - ♦ The impact of a disruptive event must be evaluated
 - **Downtime Estimation-**
 - ♦ Maximum delay businesses can tolerate and still viable
 - ♦ Estimates the MTB / Maximum Tolerable Downtim
 - ♦ Estimate the financial and operational impact
 - **Resource Requirements-**
 - **Does not recommend recovery solutions**
- **4 Steps**
 - **Identifying Resources and Systems**
 - ♦ Identify all business UNITS within the organization
 - ♦ Human Resources
 - Org Chart to determine functional relationships
 - Operators
 - Users (Data entry or analyst)
 - Can peoples get to work ?
 - Are there critical skills possessed by one person ?
 - Can peoples easily get to an alternative site ?
 - ♦ Identify Processing Capability
 - ♦ Identify Computers Based services
 - ♦ Identify Automated Applications and data
 - ♦ Identify Procedures / Documents
 - ♦ Vital Records Program
 - ♦ Identify Tasks
 - ♦ Identify Supplies
 - ♦ Identify Vendor support
 - ♦ Critical Business Units
 - ♦ Critical Support Units
 - **Perform the assessment**
 - ♦ Is smaller than a full risk assessment
 - ♦ A function is to conduct a loss impact analysis
 - ♦ Critical support areas must be defined
 - ♦ Asset identification and valuation
 - ♦ Vulnerability Assessment
 - Critical Support Areas must be defined
 - Quantitive Approcah
 - Qualitative Risk Analysis
 - **Analyze the compiled information**
 - ♦ The main goals of risk Analysis
 - ♦ Definition
 - ♦ Risk Metrics/Modeling
 - ♦ Steps of Risk Analysis
 - Assign value to information and assets
 - Estimate potential loss per Risk

- What physical damage can take place & how much that cost ?
- How much productivity can be lost and how much would that cost ?
- What is the value lost if confidential information is disclosed ?
- What is the cost of recovering from a virus attack ?
- What is the cost of recovering from a cracker attack ?
- How much would it cost if critical devices failed ?
- Calculate the single Loss Expectancy SLE
- Single Loss Expectancy [SLE]
- Perform a threat analysis
- Derive the overall loss potential per Risk [ALE]
- Choose remedial measures to counteract each risk
- TASKS OF INFORMATION RISK MANAGEMENT
- Documentation and Recommendation
 - ♦ A written plan must be developed
 - ♦ The written plan is very important
 - ♦ The written plan should include
 - Assignment of individual and team responsibilities
 - Damage assessment and containment
 - Activation of short and long term backup plans
 - Access to data backup facilities
 - Recovery of critical systems and files
 - Notification to staff, customers, suppliers
 - Availability of alternative support services
 - Restoration of primary data processing facility
 - Orderly resumption of moving back to main site for operations
 - ♦ The plan should have four phases
 - Activation
 - Restoration
 - Testing
 - Maintenance

❖ Plan Approval and Implementation

- **Approval by Senior Management**
- **Creating awareness - training and awareness enterprise wide**
- **Maintenance of the plan - plans get outdated quickly**
- **DRP and BCP should be tested at least EVERY Year**
- **Reasons Plans Become Outdated**
- **Ways to Keep the PPlan Updated**
 - **Make DRP and BCP part of every business decision**
 - **Insert the maintenance responsibilities into job descriptions**
 - **Include maintenance in personnel evaluations**
 - **Perform internal audits that include DRP and BCP**
 - **Perform regular drills that use the plan**

❖ BCP Definitions

- **Names given to BCP**
 - **Disaster Recovery**
 - **Business Continuity Planning**
 - **End-user Recovery Planning**
 - **Contingency Planning**

- Emergency Response
- Crisis Management
- **BCP is when a man-made or natural event is minor**
- **Deals with a longer look of the problem than disaster recovery**
- **BCP is about making the plan and the framework**
- **BCP is enterprise wide**
- **Created to prevent interruptions to normal business activity**
- **Should be part of the security policy program**
- **Minimize the effect of impact and allow resumption of business process**
- **Requires involvement from many personnel**
- **Availability Integrity and confidentiality needs to be considered**
- **The most critical piece is management support**
- **Planning can take up to 3 years**
- **Reasons for BCP**
 - **Should be Considered at every phase of system SDLC**
 - **Should Address Residual risks**
 - **Proactive rather than Reactive**
 - **Take the correct actions when needed**
 - **Allow for experienced personnel to be absent**
 - **Saves time, mistakes, stress and \$\$**
 - **Short and long term loss of business**
 - **Effect on customers**
 - Public image
 - Loss of life
 - **Legal and Regulatory sanctions, civil suits**
 - **Foreign Corrupt Practices Act of 1977**
 - **Standards of Due Care**
 - **BCP Information Security Goals**
 - Confidentiality/Sensitivity
 - Integrity/Accuracy
 - Availability/Recovery
 - Disclosure
 - Modification
 - Destruction
 - Denial
- **BCP Planning Cover**
 - **A data backup is the first step**
 - **Local and Wide Area Networks and servers**
 - **Telecommunications and data links**
 - **Workstations and workspaces**
 - **Applications software and data**
 - **Media and records storage**
 - **Staff duties**
 - **Number One priority is always People First!**

- **Describes procedure for**
 - Emergency response
 - Extended back up operations
 - Post recovery

➤ **BCP What Disasters to prepare for**

- **Natural Events**
 - Fires, Explosions, hazardous material spills of environmental toxins
 - Earthquakes, storms, floods, and fires from nature
 - Power outages and utility failures
- **Man Made Events**
 - Bombings Sabotage
 - Strikes, job actions
 - Employee or Operator unavailability due to emergency evacuation
 - Communications infrastructure failures
- **Technical Threats**
 - Hardware/Software Failures
 - Files corruption
 - Backup corruption
 - Loss of a T1 line
- **Threats**
 - Errors & omissions 50%
 - Fire, water, electrical 25%
 - Dishonest employees 10%
 - Disgruntled employees 10%
 - Outsider threats 5%

➤ **Four Prime Elements of BCP**

- **BIA is performed at the Beginning of BCP and DRP**
- **Scope and Plan Initiation**
 - Marks the beginning of BCP process
 - Identify threats from both internal and external sources
- **Business Impact Analysis**
 - Used to help business understand the impact
 - Include Vulnerability Assessment
- **Business Continuity Plan Development**
 - Use BIA results to develop the BCP
 - Include Plan Implementation
 - Include Plan testing
 - Include Plan maintenance and Update
- **Plan Approval and Implementation**
 - Getting final management approval
 - Creating enterprise-wide awareness
 - Implement plan Update Procedures

➤ **Assessment Types**

- **Business Impact Analysis (BIA)**
 - Assessment of an organization's business functions
 - Develop an understanding of their criticality
 - Understand the Recovery time & objectives

- Evaluate the resources needed
- Help Understanding the impact of a disruptive event
- **Risk assessment**
 - Reduce risks to an acceptable level
 - Evaluation of the exposures present
 - Focus risk management efforts and resources
- **Business Assessment**
 - Risk assessment + BIA
- **Disaster recovery plan**
 - Actions to be taken before, during and after a disruptive event
- **Risk Management**
 - Includes the risk assessment
 - Determination of suitable technical, management, and operational controls
 - Developed in anticipation of a possible event
 - Executed after that event has occurred
- **Occupant Emergency Plan (OEP)**
 - Provides the procedures for occupants of a facility (When life is at risk)
 - Developed at the facility level
 - Specific to the geographic location and structural design
- **Continuity of Operations Plan (COOP)**
 - Required by Presidential Decision Directive 63
 - For sustaining an organization's (headquarters for 30 days)