Business Continuity Management

CliftonLarsonAllen

cliftonlarsonallen.com

Introductions

- Brian Pye
  - CliftonLarsonAllen – Senior Manager
  - Business Risk Services group
  - 15 years of experience with Business Continuity
- Megan Moore
  - CliftonLarsonAllen – Senior Manager
  - Business Risk Services group
  - 9 years of experience with Business Continuity

Session Objectives

- Why is it Important
- Define Business Continuity
- Getting Started and Objectives
- Content of a Plan
- Responsibilities and Objectives
- Business Continuity Life Cycle

Why is Business Continuity Important?

- Increased dependence for businesses on IT;
- Reliance on business-critical information;
- Importance of protecting irreplaceable data;
- Most foundations relying on their computer systems as critical infrastructure in their business;
- Most foundations do not have a comprehensive business continuity or disaster recovery plan

It Can Happen and DOES Happen!

- According to the Federal Emergency Management Agency (FEMA), in 2011, 80 presidential declared disasters have occurred
  - 55 severe storms
  - 12 tornado
  - 5 flood
  - 3 earthquake
  - 5 other
- FEMA estimates that upwards of 70% of organizations in the country will experience some form of operational disruption due to severe storms, tornadoes and flooding
- Most organizations only spend between 2% and 4% of their IT budget on disaster recovery planning;
- Of companies that had a major loss of computerized data without a disaster recovery plan:
  - 43% never reopen;
  - 51% closed within two years;
  - only 6% will survive long-term

What Should We Be Thinking About?

- What state would my business be in if we experienced one of these events?
- How long would it take for me to recover?
- Define all of the efforts needed to get us back in operation?
  - Information technology based
  - Operation based
- How much revenue would we lose if we were “down” for 24, 48, 72 hours?
- How safe are my foundation’s assets?

What is Business Continuity Planning (BCP)?

- BCP is the process whereby foundations ensure the maintenance or recovery of operations when confronted with adverse events including:
  - Natural disasters
  - Technology failures
  - Human error
  - Terrorism
- The objectives of a BCP are to minimize financial loss, continue to help consumers, and mitigate the negative effects that disruptions can have on strategic plans, reputation, operations, etc.

Getting Started

- Define some important terms and metrics for business continuity planning
  - What is a disaster
  - Key business processes
  - Business critical systems and data
  - Recovery Point Objective (RPO)
    - ◊ Defined as the amount of data lost measured in time.
    - ◊ Example: If the last available good copy of data upon an outage was from 24 hours ago, then the RPO would be 24 hours.
  - Recovery Time Objective (RTO)
    - ◊ Defined as the duration of time and a service level within which a business process must be restored after a disaster in order to avoid unacceptable consequences associated with a break in continuity.

What are the Objectives?

- A BCP should reflect the following objectives:
  - BCP is maintaining, resuming, and recovering the overall business, including the recovery of technology (disaster recovery).
  - The planning process should be conducted enterprise-wide and include all functional departments.
  - A thorough business impact analysis and risk assessment are the foundation of an effective BCP.
  - The effectiveness of a BCP process can only be validated through testing or practical application.
  - The BCP and test results should be subjected to an independent audit and reviewed by the board of directors.
  - A BCP should be periodically updated to reflect and respond to changes in the Foundation or its service provider(s).

Business Continuity Planning Content

- Overview
- Policies and preparedness
- Organization impacts
- Notification strategy / plan activation
- Business process continuity roadmap
- Personnel dependencies / succession
- Technology infrastructure
- Facility and space

Who is Responsible?

- Senior management is responsible for:
  - Allocating sufficient resources and knowledgeable personnel.
  - Development of the BCP.
  - Setting policy by determining how the foundation will manage and control identified risks.
  - Review BCP test results.
  - Ensuring the BCP is kept up-to-date and approved on an annual basis.
  - Employees are trained and aware of their role in its implementation.

Business Continuity Planning Lifecycle

- Analysis
- Solution design
- Implementation
- Testing and acceptance
- Maintenance

Analysis Phase

- Define the team
- Identify your key business processes
- Initiate the planning process
  - Impact analysis
  - Threat analysis
  - Recovery requirements (business & technical)
- Compile your business continuity manual

Analysis Phase

- Business Continuity Manual
  - May be simply a printed manual stored safely away from the primary work location containing:
    - ◊ The names, addresses, and phone numbers for crisis management staff;
    - ◊ General staff members;
    - ◊ Clients and vendors;
    - ◊ Insurance contracts;
    - ◊ The location of the offsite data backup storage media;
    - ◊ Data/systems recovery process
- Include recovery requirements
  - Number and types of workstations
  - Primary and secondary locations
  - Key individuals involved in a recovery effort
  - Key applications and date
  - Maximum time allowed for an outage
  - Peripheral requirements like computers, printers, copiers, faxes, etc.

Business Impact Analysis

- A business impact analysis (BIA) is the first step in developing a BCP. It should include the following:
  - Identification of the potential impact of uncontrolled, non-specific events on the foundation's business.
  - Consideration of all departments and business functions, not just data processing.
  - Estimation of maximum allowable downtime and acceptable levels of data, operations, and financial losses.

Risk Assessment

- A risk assessment is the second step in developing a BCP. It should include the following:
  - Prioritizing of potential business disruptions based upon severity and likelihood of occurrence.
  - A gap analysis comparing the existing BCP, if any, to what is necessary to achieve recovery time objectives.
  - An analysis of threats based upon the impact on the Foundation, including its consumers, not just the nature of the threat.

Solution Design Phase

- Your goal is to identify the most cost effective disaster recovery solutions based on RPO and RTO based on your foundations risk tolerance levels.
- Develop critical response times and recovery strategies.
- Important ranking of key business applications and processes:
  - E-commerce;
  - E-mail based communications;
  - Production processes;
  - IT services;
  - Finance;
  - Sales and marketing;
  - Accounting & reporting;

Implementation Phase

- Complete assessment of your IT and operational infrastructure;
  - Significant operational processes
  - Network (communications and security equipment)
  - Servers
  - Workstations
  - Application systems
  - Data files and databases
- Review the findings report (health check);
- Make the necessary improvements;
- Document the new environment.

Testing and Organizational Acceptance Phase

- Test the plan in it entirety or parts
  - Power outages
  - Hardware failures
  - Telecommunications outages
  - Applications test
  - Business process test

Notification Strategy & Plan Activation

- Who to call
- When to call
- Assessment….how extensive is the damage?
- Plan activation…..yes or no?

Maintenance Phase

- Monitoring is the final step in business continuity planning. It should ensure that the Foundation's BCP is viable through the following:
  - Testing the BCP at least annually.
  - Subjecting the BCP to independent audit and review.
  - Updating the BCP based upon changes to personnel and the internal and external environments.
  - Perform training.

Important Notes

- Firms should ensure that their BCP manual is realistic and easy to use during a crisis;
- The BCP sits along side crisis management and disaster recovery planning and is a part of a foundation's overall risk management.

Best Practices

- Implement a back-up and data restore process.
- Due to power outages…
  - Implement a battery back up solution and surge protection strategy;
  - Consider a diesel generator for your data center of facility;
- E-mail application defense….
  - Spam and viruses filtering before they enter your network;
  - Keep your desktops, laptops and mobile devices secure from viruses and theft
- The BCP sits along side crisis management and disaster recovery planning and is a part of a foundation's overall risk management

Brian Pye
Senior Manager Business Risk Services
Brian.Pye@cliftonlarsonallen.com
612-397-3139

Megan Moore
Senior Manager Business Risk Services
Megan.Moore@cliftonlarsonallen.com
612-397-3129