Testing Methodologies
For
Validating Business Continuity Plans

Compiled by

SIFMA Business Continuity Planning
Committee
Best Practices Subcommittee

Published January 2008

Introduction

The effectiveness of a firm's business continuity program is critical to the success of a firm's recovery effort when faced with a business disruption. Exercising, or testing, is the most effective way to determine the validity of a plan and its capacity to meet the firm's objectives.

This document has not been tailored to fit any particular business practice or infrastructure environment and CANNOT alone satisfy any particular firm's regulatory requirement or need for a continuity program. Each firm must analyze its own circumstances and design a continuity program designed to address its own risks and dependencies. This document provides information on areas to consider when validating a business continuity plan and suggests some possible methodologies to use to measure the capabilities of the plan. This guideline is not designed to be an exhaustive set of procedures that organizations must follow to assess the capabilities of their business continuity plans. Since various methods may be used to validate a business continuity plan, omission of any particular tests or practices suggested in this document does not suggest a failure to properly analyze or validate a business continuity plan, and reliance only on the tests or practices suggested herein cannot assure a complete and effective business continuity program. Each firm must exercise its own judgment when determining which procedures are appropriate for its specific organization.

Why test business continuity plans?

Business continuity plans are tested and exercised for a number of reasons. It's also valuable to install a process that allows the organization to track, report, correct and retest deficient components.

- Measure capabilities under different scenarios and determine if the plan is effective
- Identify gaps in documentation and planning
- Determine if the firm is prepared to meet the challenges of a crisis
- Uncover weaknesses and highlight strengths
- Ensure compliance with regulatory requirements
- Validate the resources required to meet stated objectives
  - People
  - H/W (spell-out) and capacity
  - Telecom
- Ensure tools work as required
- Ensure external parties can support organizations needs "at time of"
  - Transportation
  - Voice and Data
  - DR (define) Providers
  - Offsite Vaulting
  - Catering
  - Equipment and Service Company
  - Etc.
- Ensure participants or recovery teams understand their role with each scenario
- Ensure organizational structure accommodates capability to maneuver
  - Management is prepared
  - Business lines are prepared
  - IT is prepared
- Instill confidence in executive management, regulators, the Industry, and our clients

What areas may be tested for validation purposes?

The success of a Business Continuity Program is dependant on various components working together to achieve a common goal. Depending on the nature of the business, the areas listed below may be considered when planning the firm's testing.

- Crisis Management
    - Safety and Security of the Staff
        - Communications Plans – Internal and External (i.e., Media)
        - Emergency Notification Systems
        - Evacuation Plans
        - Shelter in Place – Short Term and Long Term
        - Contacts and Coordination with local government offices (i.e., Police, Fire, Health, Office of Emergency Management)
    - Survival of the Business
        - Core Critical Infrastructure
        - Regulatory Required Systems/Applications/Services
        - Recovery Teams and Procedures
        - Transportation Services "at time of"
        - Damage Assessment capabilities and supporting vendors
- IT Disaster Recovery
    - Ability to meet expected RTOs and RPOs (spell out or define at first use)
    - Recovery Procedures
    - Voice and alternate voice capabilities
    - Telecom Infrastructure
    - Desktop Recovery
    - Offsite Storage Delivery and Response
    - Mobilization of IT Support
- Business Continuity Plan
    - Calling tree – Contact information and procedures
    - Recovery Team Roles and Responsibilities
    - Activation of the plan
    - Coordination with Counterparties, Agencies, Regulators

- Dependencies interdepartmental locally and abroad, if applicable
- External dependencies
- Mobilization of Staff to the Recovery Site
- Recovery Operating Procedures
- Access to non-standard supplies, (i.e., Preprinted tickets, statements, checks, etc.)
- Connectivity
- Desktop Applications and Tools
- Transportation and Lodging

What methodologies can be used to validate plan components?

Following are techniques that can be used to exercise each component of the business continuity program. Planning, coordination, execution, reporting and follow up are important elements of a comprehensive validation program.

- Tabletop Exercise – Great benefit, least amount of coordination
  - Can be used in each of the 3 main areas: Crisis, IT, Business Continuity
  - "Thought Provoking" Process to work through different scenarios
  - Include multiple departments, external partners, global partners
  - Develop scenarios to stress specific parts of the plan
  - Can be conducted onsite during business hours – 2hrs to 8hrs
  - No technology involved
  - Role play, teamwork
  - Be flexible to change the flow of the scenario if necessary
  - Document findings and have all departments update plans from results
  - Low risk level

- IT Testing
  - Focus on IT only
  - Can be conducted with or without business participation to validate
  - Can be conducted during business hours
  - Single system or component testing
  - Connectivity Testing
  - Document procedures and use to execute tests
  - Include 3rd party and agencies for connectivity testing and coordination
  - Groups of systems/applications for a business line
  - Use minimal resources to validate Recovery Time and Point Objectives
  - Voice redirection internal and external
  - Telecom switching
  - Medium risk if conducted during business hours

- Full Scale Business Continuity Exercise
  - Conducted during weekend
  - Various scenarios considering midweek, midday and overnight failures
  - Major planning and coordination effort
  - Comprehensive and complete
  - Very difficult
  - All mission critical systems, internal and external are tested at same time
  - Full IT and Business participation
  - RTO and RPO validation
  - Validate site and/or 3rd Party capabilities
  - High level of risk

- Full Integration Testing with Business and IT
  - Conducted during normal business hours
  - Major planning and coordination effort
  - Most comprehensive and complete
  - Most difficult
  - Full IT and Business participation
  - RTO and RPO validation
  - Validate site and/or 3rd Party capabilities
  - All mission critical systems, internal and external are tested at same time
  - Staff relocated to alternate site to perform normal business tasks using BC Plans
  - Highest level of risk