



Turning the Top 10 Deficiencies in Today's BCPs into Program Enhancements

Paul L. Striedl, CBCP

Business Continuity Professional, MITRE

CEO/Chairman, Association of Contingency Planners (ACP)

Agenda

■ Top Ten Deficiencies / Remedies

- Confusing the BC Program with the BC Plan
- Poor design / layout
- Improper RTO prioritization
- Recovery Strategies inconsistent w/BIA findings
- Lack of an Incident Management structure
- Not completing vendor/third party risk analysis
- Non-existent or invalid testing/exercising
- Lack of alternate sites for business units
- Lack of team task lists
- Lack of BCP Executive Sponsorship

■ How Do I Perform A Plan Assessment?

Issue One

- **Confusing the Business Continuity Program with the Business Continuity Plan**
 - The BC Program should be a comprehensive “how to get there from here” multi-phased management activity. It includes such things as the “philosophy of planning”, risk assessments, corporate policies and procedures, the comprehensive BIA and Recovery Strategies Analysis
 - While these document important concepts and support, many are of little/no value at time of disaster
 - Having to weed through these documents in time of disaster dilutes the Plan’s effectiveness by providing too much information at a time when it is not needed
 - The BC Plan is the “cookbook” to use at the time of the disaster
 - The quick and dirty who, with what, where, when, and how that was derived as a result of the BC Program
 - Action verbs and activity checklists

Issue Two

- **Business Continuity Plans are “hand-cuffed” with a poor manual design and layout**
 - Illogical Flow
 - Confusing layout
 - Cumbersome (Did you pay by the page/pound?)
 - Bigger isn't necessarily better in BCP
 - Remember, the BCP is your “cookbook” to be used to respond to an incident
 - Can you follow the guidance in the plan as you would a recipe?
 - Should some key personnel be unavailable, could someone not totally familiar with it be able to muddle through?

Issue One and Two - Remedy

■ Streamline your plans to include:

- **Introduction (aka audit food)**
 - Objectives, Purpose, and Scope
 - Overview of plan structure, general strategies, and BC Organization (in other words, an “executive summary” and how to use this document)
 - Incident Command Team “big picture”
- **Contact Information**
 - Team Members and Call Tree
 - Vendors / Clients / Other critical contacts
- **Functions**
- **Task/Activity checklists**
- **Resource Requirements (over time) - What, how many, by when**
- **Vital Records (e.g., Off-Site Storage Items, Floor plans, SOPs, contracts, etc.)**
- **Exhibits (directions to alternate sites, etc.) and forms**
- **Anything else deemed “necessary” by audit / regulators**

Issue Three

- **BIA Defines Recovery Priorities solely by department**
 - Two common ways this occurs:
 - RTOs established by departments/groups vs. globally (across the enterprise), not taking into account interdependencies and economies of scale
 - Viewing the department as a whole vs. by select function
 - Some Call Center functions might require a Recovery Time Objective (RTO) of a few minutes, but many other intra-departmental functions can be delayed for days, weeks, months.) It is unlikely that the ENTIRE department is needed to perform all critical processes
 - Routine functions (e.g., training, quality control and reporting) could tolerate longer recovery timeframes, allowing the organization to focus on other critical priorities
 - Overly stringent RTOs can place the organization at risk by over obligating resources and can result in unnecessary expense

Issue Three - Remedy

- **Reexamine BIA and define priorities by functions (input/output analysis)**
- **Create tables to:**
 - Summarize RTOs across the enterprise (department function / application)
 - Provide RTOs by Business Function (lowest to highest)
 - Provide minimum RTOs by IT application (lowest to highest)
- **Have senior management validate results**
- **Don't "fall in love" with your RTOs**

Issue Four

- **Business Impact Analysis contradicts the defined Recovery Strategies**
 - The RTOs should drive the recovery strategies
 - If there is a defined a RTO of 2 hours for critical IT systems and a drop-ship solution strategy requiring 24 hours for delivery is adopted, it is impossible to meet the RTO. Therefore this is NOT a viable recovery strategy
 - Recovery Strategies should be tailored so that their implementation will ensure the RTOs are met

Issue Four - Remedy

- **If the Recovery Strategy does not fit the RTO...**
 - The recovery strategy must be revised so that its adoption will allow the RTO to be met. Remember, the RTO is the driver and validates that the recovery strategy is indeed appropriate and suitable
 - Much comes down to the amount of risk management is willing to assume. If budgetary constraints are such that management chooses to hedge its bets, then such needs to be documented as an exception to the RTO/Recovery Strategy recommendations

Issue Five

- **Lack of an Incident Management Team Structure / Disaster Declaration Process**
 - The purpose of this team is to manage the disaster from a strategic perspective and provide direction for the recovery teams (Damage Assessment, Executive Emergency, Department/Group Recovery, and Restoration). Its existence is paramount. Not having this team leaves the recovery effort “headless”
 - In addition to not having an IMT, some firms also lack a formal disaster declaration procedure, which is needed as a trigger point and for insurance claim information and processing

Issue Five - Remedy

■ Create Incident Management Team / Plan

- Who is on the team?
 - Typically shared services departments (Security, Facilities, HR)
- Who is the incident manager/commander?
- Who are the primaries and alternates?
- How are team members notified?
- Where is (are) the command center(s)?
- What are the team's responsibilities?
 - General responsibilities
 - Specific activity/task list

■ Document the disaster declaration process

- Who is authorized (primary and alternates)?
- Definition as to what constitutes a disaster

Issue Six

■ Lack of a comprehensive Testing Strategy

- Some BCP Programs limit their testing to the IT arena, excluding the business units, operational and back-office functions
- Tests are too “easy” and often retest areas known to “pass.” The time to find flaws in your plan are during testing, not during a disaster. If you’re not finding something that can be improved, you’re not testing hard enough!

Issue Six - Remedy

- **Create a comprehensive testing strategy to involve a greater cross-section of organizational personnel**

- **Tests should be defined and increase in level of complexity (e.g., small group tabletop, large group tabletop, limited walk-thru/simulation, parallel testing, etc.)**

- **There are several other types of exercises which can be conducted, such as:**
 - checklist tests (tabletops)
 - call tree exercises
 - structured walk-throughs
 - disaster simulations

Issue Seven

■ Alternate Sites Not Identified for All Business Units

- Some plans identify the location for IT recovery but do not address alternate workspace for the business units and other supporting functions
- While having a home for the IT recovery is paramount, an IT infrastructure supports the business and has little value when end users are unable to access their data

Issue Seven - Remedy

- **Analyze required resources (work space) over time**

- **Determine if internal recovery is possible / feasible**
 - Conference Rooms / Training Rooms
 - Cafeterias
 - Non-critical departments (can they be displaced?)
 - Work in Shifts
 - Other company facilities (warehouses, sales offices)

- **If there is no internal solution, look external**
 - Hot Sites, Mobile Recovery, and Telework

Issue Eight

■ Lack of a Team Task Lists

- Many BCPs do not have a prioritized task list which documents what to do first, second, third, etc. in a disaster situation. Remember the “cookbook”
- Most important component of the plan
- Provides the “recipe” of how to recover

Issue Eight - Remedy

- **There are two types of team task lists**
 - Generic (better than nothing, but not everything you need)
 - Team specific
 - Conduct brainstorming sessions to identify what you would do after notification of an event
 - Write tasks from the perspective of someone with a similar skill set performing the task. Minimize dependency on institutional knowledge of key personnel
- **Document team task lists in checklist form (Again with the cookbook/recipe) and make sure it is printed and stored in multiple locations**

Issue Nine

- **No analysis of vendor and third-party “outsourced functions” risk**
 - Critical vendors supply inputs into critical business functions and affect RTOs
 - Outsourced functions perform the entire business process
 - SLAs and force majeure
 - Risk might be greater if they have the disaster
 - BCP cannot be restricted to the silos of your own company
 - No organization is 100% self-sufficient

Issue Nine - Remedy

- **Take an inventory of relationships at least once per year**
- **Initiate a process of distributing vendor endorsement letters to understand delivery timeframes of key supplies**
- **Request and review all third-party BCPs and BCP testing documentation**
- **Conduct analysis and provide findings to senior management**
 - Suggest alternate vendors if necessary

Issue Ten

- **Lack of business continuity executive sponsorship**
 - Many organizations do not have senior management involvement in the creation and ongoing BCP process
 - High level exposure and senior management support is VITAL to the successful development of a business continuity capability
 - If the the C Level isn't driving BCP, who else will?
 - Executive sponsorship enforces the commitment to the corporate mission

Issue Ten - Remedy

- **Create BCP Steering Committee to act as:**
 - Advocate
 - BCP expert
 - Consultant
 - Auditor
 - Evaluator

- **Conduct quarterly meetings and document minutes**

- **If senior management is not supportive, advise internal audit**

How Do I Perform A Plan Assessment?

- **Hire an independent BCP consultant to perform an expert and unbiased review**
 - Expect to pay \$155-\$310 (per hour) plus expenses per consultant

- **Utilize relationships in BCP networking groups (plan swaps)**

- **Perform your own assessment using benchmarks**
 - FFIEC (banking)
 - Business Continuity Maturity Model (Virtual Corp.)
 - BCI Standard PAS 56
 - NIST 800-53
 - NFPA 1600

Any questions?

**Paul L. Striedl, CBCP
Business Continuity Professional
MITRE**

**703-983-1447 (office)
703-220-3604 (cell)**

pstriedl@mitre.org