

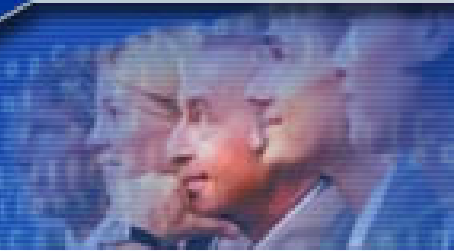
Conducting a Business Continuity Plan Audit



BY TED BROWN, CBCP CBCV
PRESIDENT & CEO
KETCHCONSULTING
MEMBER CPM HALL OF FAME



 *KETCH Consulting*™



KETCHConsulting: WHAT DO WE DO?

- Executive Justification of Business Continuity
 - Analyze your ROI
 - Create/give executive presentations
- Hot Site Contract Negotiations
 - Current/Future Pricing
 - Length of Contract
 - Ts & Cs
 - Quantity/Quality/Scheduling of test time
 - Termination clauses
 - Guarantees
- Alternate Site Strategies, Solutions, and Costing – we give you choices
- Risk Assessments
 - Observational
 - Statistical
 - Supply chain
- Disaster Recovery Plans
 - Technology Recovery
- Work Place Violence Planning
- Business Continuity Program Development
 - People plans, not just technology
- Develop/enhance/assess/update your Business Continuity Plan
- Gap Analysis
 - Analyze the difference between the plan and reality
 - Develop a new plan
- Business Impact Analysis
 - Identify and quantify direct and indirect risks, and resultant business impact of these risks, to your core business processes
- ICT (NIMS)
- Helicopter & Jet Evacuation plans
- Table Top exercises
- Swine Flu



KETCHConsulting: WHAT MAKES US DIFFERENT?

- Leadership
 - Actual Recoveries
 - Speakers at all major conferences
 - Published-authors of hundreds of articles
- Quality of staff
 - Experienced professionals that average 30 years in IT and 20 YEARS in BCP
 - Trained in, and in some cases, innovators of, the top methodologies in the industry.
 - All consultants are certified (CBCP/MBCI).
 - Heavy experience in designing, developing, testing and executing successful recovery plans. "We know what makes them work!!"
- Hot Site Negotiations
 - First Hand knowledge of where cost savings can be realized & what T's & C's really mean
 - Guaranteed savings
- Packaging Consulting Solutions with:
 - Full spectrum of offerings can be "packaged" to provide a single cost effective solution
 - Hardware, software, data center equipment, hot site, financing
 - "Roll your own deal"
- Price Competitive
 - Low Overhead
 - Leverage
 - Packaging



Why Worry?

According to a recent survey, **37** percent of chief financial officers (CFOs) perceived their firms to be most vulnerable in the area of disaster preparedness and recovery.



The Auditing Dilemma

Unlike finance, there are no “generally accepted principles” with which to analyze business continuity plans.

There are, however, a number of questions auditors can ask to help evaluate a firm’s business continuity plans.



Disaster Recovery vs. Business Continuity

- *Disaster Recovery historically focused on recovering technology thus Hot Sites, Alternate Sites, Quick Ship, and Mobile Recovery Centers were developed.*
- *Since the 1990's, the focus has been on Business Continuity, not just technology recovery. This is even more true since Sept. 11 and Katrina. Information Technology (IT) is a subset of Business Continuity*



1. What are the BC objectives?

- Are the objectives specific?
- Are they measurable?
- Are they endorsed by senior management?

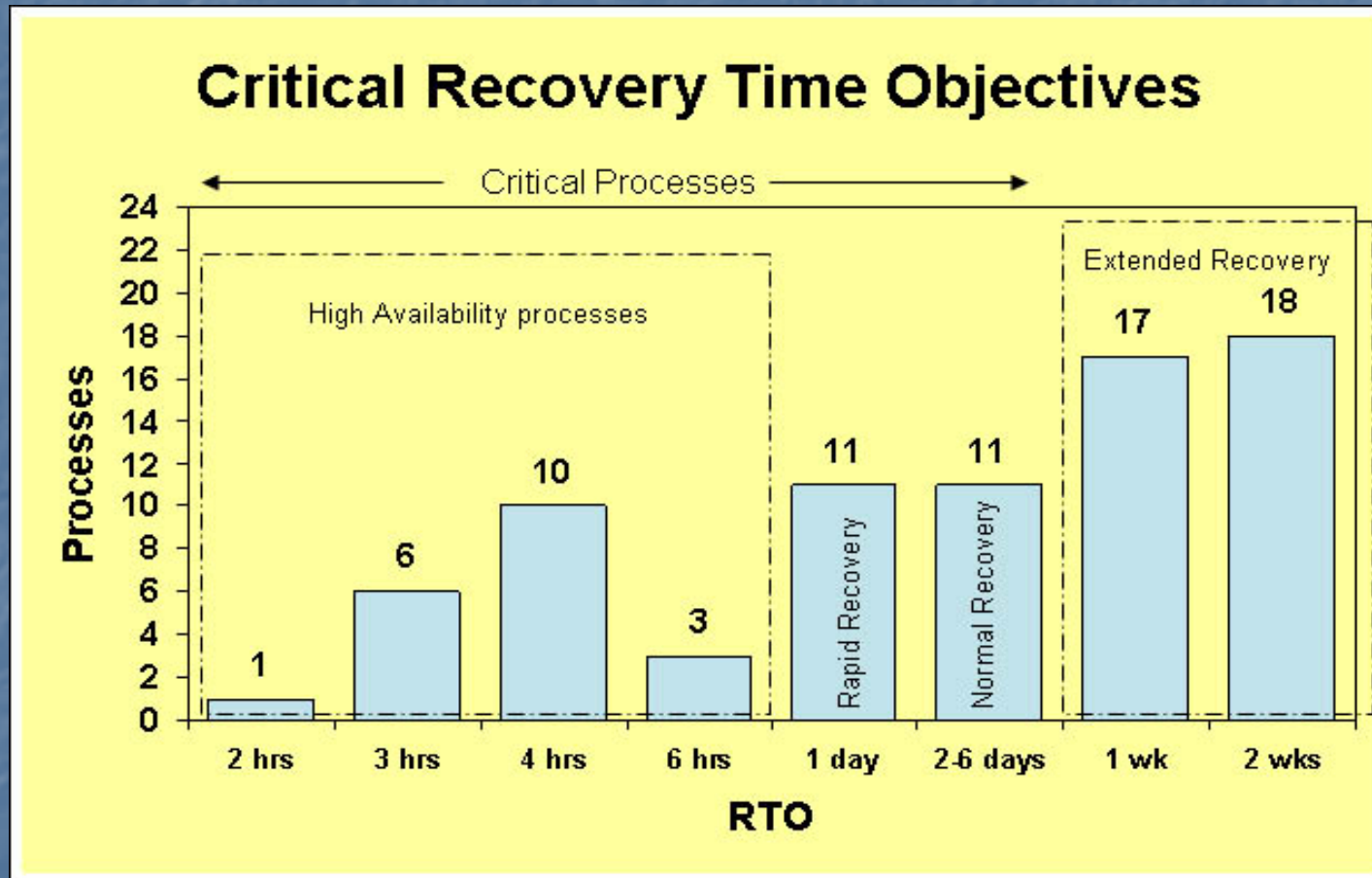


2. Are the BC objectives realistic?

- If the goal, for example, is to re-establish full operations within 24 hours, can the goal be achieved?
- If not:
 - Should the recovery window be expanded?
 - Should the plan be amended to achieve the 24-hour objective?



Critical Recovery Time Objectives



3. Is BC relevant to employees?

- Are employees aware of the business continuity plan?
- Did they have input into plan development?
- Do they understand their obligations under the plan?
- Are they comfortable with their current level of training?
- Do they have any reservations regarding plan execution—or viability?



4. When was the last BIA?

The Business Impact Analysis (BIA) is the template for developing a business continuity plan.

A BIA should be conducted at regular intervals, or coincident with any major business or organizational change.



5. Is BC tied to change?

A business continuity plan should be reviewed and revised coincident with any major business or organizational change, for example:

- The opening of a new office.
- The introduction of a new product line.
- The passage of a new government regulation



6. Is the BC plan tested?

- Are tests conducted on a regular basis?
- Are the tests comprehensive?
- Are all problems revealed by the tests resolved?
- Are appropriate changes made to:
 - The business continuity plan?
 - The business continuity test protocols?



7. Are offsite backup tapes tested?

- Backup media may degrade over time.
- Backup procedures may fail without notice.
- Backup volumes should be randomly retrieved and restored to ensure the integrity of the backup process.



8. Is the BC plan detailed?

- Primary recovery personnel may not be available in the wake of a disaster.
- Can the business continuity plan be executed by backup recovery personnel, i.e., non-experts?



9. Is the recovery site secure?

- Suffering a disaster does not absolve a firm from its security obligations.
- How secure is the recovery site?
 - Physical security?
 - Information security?
 - Personnel security?
 - Transportation security?



10. Where is the 2nd recovery site?

- Like airlines, recovery site providers “overbook”.
- If the primary recovery site is taken, where is the secondary recovery site?
- Is it logistically—and economically—feasible to operate from the second site?



11. What about “telework”?

- Today, most employees have home computers with Internet access.
- Does the business continuity plan provide for telework-oriented recovery strategies?



12. What if business partners fail?

Does the business continuity plan:

- Provide for periodic audits of business partner business continuity plans?
- Include recovery plans designed to mitigate the impact of a major business partner failure?



13. What about hardcopy data?

- All business continuity plans provide for the recovery of computer data.
- What about vital paper or hardcopy records?
- Is document imaging available for those who wish to use it?



14. What about Pandemic?

- Is there a separate module for a Pandemic?
- Are triggers tied to WHO and CDC?
- Have HR policies been defined?
- Have travel plans been defined?
- Is there a plan for anti-virals?
- Have employees been educated?



15. What about non-IT assets?

- Virtually all business continuity plans provide for the restoration of IT assets.
- What about non-IT assets, such as:
 - Manufacturing plants?
 - Vehicles and equipment?
 - Research and development laboratories?
 - Raw materials?
 - Product inventory?



16. What about risk mitigation?

- Since not all disasters can be avoided, part of the business continuity plan should be devoted to lessening their impact.
- Strategies include:
 - Decentralization of critical assets.
 - Diversification of key vendors.



17. Are “disruptions” covered?

Does the business continuity plan provide for lesser disasters, such as:

- Power outages?
- Loss of key personnel?
- Denial of service attacks?
- Work stoppages?
- Loss or theft of mobile computing devices?



18. Are EM plans integrated?

Does the business continuity plan integrate other, related emergency management plans, such as:

- Evacuation?
- Shelter In-Place?
- Emergency Medical?
- Crisis Management?



19. Are all executives on board?

- Does the business continuity plan enjoy the support of senior management?
 - Financial support?
 - Promotional support?
- Are employees held accountable for their business continuity performance?



20: Is the plan readily accessible?

- Are current copies of the plan kept offsite?
- Are up-to-date contact lists stored in a secure location?
- Are plan updates automatically distributed to plan holders?



Conclusion

- Corporate Auditing should be proactive in evaluating their firm's business continuity plans.
- They should insist that plans encompass both IT—and non-IT—functions and assets.
- They should demand the same level of professionalism and due diligence from business continuity managers that they demand from finance managers.



CALL TEDDY:

Ted Brown, CBVP CBCV

President and CEO

1- 570-563-0868

TedBrown@KETCHConsulting.com

PO Box 641
Waverly, PA 18471
USA



 **KETCH Consulting**™

