

# Business Continuity Planning: A Risk Manager's Agenda for Operational and Credit Risk Management

by Joel Lanz

**T**his two-part article identifies current actions that risk managers need to take to strengthen their business continuity strategies. Part I focuses on operational risk management strategies for bank service delivery. Part II, to be presented in a future issue, discusses how lenders should evaluate their customers' continuity plans to mitigate the risk of a customer not meeting credit obligations due to a business interruption.

**M**any bank risk managers are in the process of reassessing business continuity risk strategies at both the operational and credit risk levels. At the operational risk management level, the strategies must ensure that customer service delivery commitments and objectives are achieved. At the credit risk management level, they must ensure that business interruptions affecting the customer's business will not affect the quality of the credit.

## Why Reevaluate Continuity Planning at the Operational Risk Level?

Given the trust and expectations of the public, banks have always played a leadership role in continuity planning by:

- Providing emergency financial assistance, including loan programs and funds to disaster areas.
- Providing "thought leadership" and sharing best practices on developing Y2K contingency plans.
- Involving the board of directors in annually reviewing continuity plans, including

incorporating recommendations from such independent experts as banking regulators and both internal and external auditors.

- Demonstrating the resilience of the industry in the aftermath of September 11.<sup>1</sup>

Recent events have changed the assumptions we make about potential events and their impact on the business that drives the continuity plan. Figure 1—taken from the FFIEC's *IS Examination Handbook*—contains the typical steps involved in the development of a corporate contingency plan.<sup>2</sup>

© 2002 by RMA. Lanz, a former Big 5 partner, leads a CPA practice that focuses on providing technology risk management services to banks; he is also an adjunct faculty member of the School of Computer Science and Information Systems at Pace University.

Note the effect that assumptions and business impact analysis-related steps (items 1-4) have on the development of the plan.

### Changing Assumptions

Banks have always tailored the assumptions used to develop a business continuity plan to their unique circumstances and considered probability of occurrence, as well as to the cost benefit of the control. Many assumptions used in plans leveraged lessons learned from Y2K compliance efforts. Additionally, as banks conducted various testing exercises, they reconsidered assumptions used and made the necessary adjustments. Three current factors placing pressure on banks to reevaluate their continuity plan assumptions are recent global events, new business and service delivery

models, and increasing use of service providers and vendors.

**Recent global events.** These events have triggered a number of revised assumptions:

- **Greater consideration given to whether the bank might fit a terrorist target profile.** Risks include but are not limited to:

- location of bank facilities and projects, especially in areas with major financial, political, or industrial activities;
- types of services provided, including having customers who may fit a terrorist target profile;
- image of the bank, especially if viewed as an icon of American prosperity; and
- conducting operations at or near landmark buildings and surrounding areas.

- **Greater potential for critical public infrastructures (for example, utilities, transportation, public safety) to be unavailable.** Previously, especially in areas not historically subjected to severe weather conditions, this threat was generally recognized as a very low probability. Additionally, a number of resource-challenged banks wrongly believed that if public infrastructures were unavailable, customer service delivery expectations would significantly decrease. Events have shown that public expectations (including those of the media) can even increase during disasters.

- **Expanded continuity planning actions relating to people.** Although continuity plans always prioritized the safety of personnel, many plans—especially those focused on operational recovery and not business continuity—gave minimal consideration to employees’ mental well-being or the impact of commuting to a “long-distance” recovery site over an extended period of time.

- **Forcing the issue of adequate testing.** Banks generally test their continuity plans on an annual basis. However, the extent of testing varies considerably, from a structured walk-through (reading and discussing the plan) to actually shutting down operations and attempting a recovery (banks that perform the latter typically do so over a weekend). Many experts agree that, at a minimum, a *parallel level* of testing needs to be performed. In this situation, the plan is tested without disrupting business operations. As a result, participation in the test is limited. Typically, the IT group takes a

Figure 1

### FFIEC IS Examination Handbook Organizational Planning Guidelines

1. Consider possible threats.
2. Assess impacts from loss.
3. Evaluate critical needs.
4. Establish priorities for recovery based on critical needs.
5. Determine strategies to recover.
6. Obtain written backup agreements/contracts.
7. Organize and document a written plan.
8. Document strategies and procedures to recover.
9. Develop procedures to execute the plan’s priorities for critical vs. noncritical functions.
10. Establish criteria for testing and maintenance of plans.
11. Determine conditions and frequency for testing.
12. Establish procedures to revise and maintain the plan.
13. Provide training for personnel involved in the plan’s execution.
14. Present contingency plan to senior management and board for review and approval.
15. After approval, store a copy of the plan off-site with other reserve supplies.

leadership role (because the test needs to be done) and the service delivery people do not adequately participate (because they are too busy serving the client). The latter is not adequately prepared to provide feedback on the accuracy and completeness of the plan, nor are they familiar with what to do in an emergency.

- **Leveraging current interest in continuity planning to increase user involvement.** Previously, although highly recommended, key service delivery personnel were not extensively involved, partly because continuity planning was perceived to be a technology rather than business responsibility, and partly because of the low prioritization of these planning projects relative to other bank initiatives. Astute continuity planners have leveraged the heightened interest level and are updating continuity plans to reflect increased input from service delivery and front-office personnel.

**New business and service delivery models.** As more banks seek to be “one-stop shops” for their customers, their reliance on technology increases as well. Examples of bank products and services that rely heavily on technology and outside partners to achieve business and service delivery objectives include:

- Consumer banking: electronic bill payment and presentment; data aggregation; online lending.
- Commercial banking: foreign exchange; Internet-based cash management; point-of-sale financing.

- Trust and investment: online brokerage; 401(k) administration; mutual fund administration.

In addition to service delivery expectations and commitments, continuity plans need to incorporate the fiduciary requirements that accompany some of these products and services.

**Increasing use of service providers and vendors.** As a result of Year 2000 preparations, banks gained a greater appreciation of the impact of outside vendors and suppliers on the bank’s ability to effectively provide service delivery. Three major industry guidelines have been recently developed to help banks manage the impact of vendors on service delivery and satisfy regulatory expectations:

1. “Risk Management of Outsourced Technology Services” issued by the FFIEC on November 28, 2000.
2. “BITS Framework: Managing Technology Risk for Information Technology (IT) Service Provider Relationships,” distributed by the BITS Financial Services Roundtable.
3. “Tools to Manage Technology Provider’s Performance Risk: Service Level Agreements,” issued by the FDIC.

All three documents require that banks perform appropriate due diligence and monitoring of the vendor’s performance relating to availability and service delivery performance. Of particular note is the active management of service providers, including using metrics

to assess performance, that may not have been in use previously.

### Risk Manager’s Agenda

The first step in reevaluation of business continuity strategies is to determine how current the contingency plan is. This typically would require reviewing the plan’s assumptions (risk assessment and business impact) with key service delivery and front-office personnel. Unless the bank has an established process to maintain the continuity plan, the probability is that the plan will be somewhat outdated. The following questions can guide the risk manager to gauge the currency of the plan—each “no” response should trigger suspicion:

- Was at least a parallel level test performed within the past 12 months?
- If yes, has the plan been updated to reflect the “lessons learned” from the test?
- Does the plan contain only currently employed personnel, along with their current contact numbers and current title? (If one of the conditions is not met, the entire question should receive a “no” response.)
- Has the plan received significant review since the first quarter of 2000? (By itself, this would not indicate a problem. However, for many banks, preparing for Year 2000 was the last time they devoted significant effort to continuity planning.)
- Has a department other than information technology raised concerns about the bank’s continuity efforts? (Again, not a

problem by itself but could indicate the level of interest by business owners in this area.)

- Can key personnel (with either organizational or recovery responsibilities) access their copy of the plan within a reasonable period of time? (If not, this could indicate that the plan may not have been read recently and, if needed, updated.)
- On an ad-hoc basis, can responsible individuals describe their roles and responsibilities in a disaster accurately and completely?
- Are products/service introduced in the past six months addressed in the plan?
- Are recently issued regulatory issues addressed in the plan (for example, privacy)?

To quickly gain an appreciation of the quality of the plan, the risk manager should consider the extent to which the plan addresses some of the common mistakes found in the bank's continuity plans. As with the above, a "no" response would indicate that the plan is deficient. Considerations should include the following:

- Does the plan include public relations strategies and other crisis management initiatives (for example, a media relations strategy)?
- Are the key business managers and front-office personnel involved and supportive of the plan? (For example, it should not be only IT driven.)
- Is periodic training (for example, briefings on changes, updates, and new strategies) provided on key plan provisions?

- Has the plan been subjected to a dedicated internal or other management control audit (for example, a separate audit of the plan rather than minor consideration as part of a general control review)?
- Does the plan include the aggregation and maintenance of records for insurance claims (for example, special documents or approval processing needed to support a claim)?
- Are critical vendors (for example, core processing and telecommunications) included in the plan, and do they participate in testing (including exercising vendor continuity plans)?
- Does the plan include returning service delivery from a disaster recovery status back to a normal status?
- Does the plan address how to maintain required regulatory, technology and other operational controls during the disaster recovery period?
- Are strategies prioritized on the basis of criticality rather than organizational political influence?

Currency and quality provide the risk manager with only a general impression of how well the bank would function in an emergency situation. It is the practical aspects of the plan that will, when the time comes, differentiate banks that can successfully navigate through a disaster from those that cannot. Practical critical success factors that need to be incorporated into the plan—whether formally documented, or more importantly, incorporated into the "way things get done" at the bank include:

- **Getting the right people involved.** Perhaps this is obvious, but many banks do not devote the necessary talent to the continuity planning project. The exposure doesn't arise from not assigning "qualified" contingency planners to the project but from not getting those who know the unique aspects of the bank and the type of service that must be delivered "no matter what."
- **Expanding participation to include specialty departments, including:**
  - public relations (to help manage media and client expectations);
  - human resources (to help manage the impact both from the disaster event itself as well as from ongoing "compromises" that employees may have to endure—for example, a long recovery time requiring an extended absence or unreasonable commute from the employees home);
  - regulatory (to help ensure that all key requirements are being adhered to despite the use of alternative facilities);
  - insurance/risk management (to maximize recovery form claim opportunities);
  - auditing (to provide an external perspective and leverage knowledge/experience available from professional institutes; access to the audit committee helps ensure that senior directives related to continuity planning are being adhered to).
- **Including continuity planning as a key component of the**

service delivery process. This includes incorporating continuity risk into the bank's change management process both on an immediate and longer-term basis. An example of each includes:

- designating—and, where possible, automatically scheduling as part of daily operations—required backup and transfer of documents to appropriate storage. In some critical situations, duplicate documents are produced (or immediately stored in a digital imaging system) at the time of transaction origination.
- for new products, services, and systems. When a new service is developed or modified, its continuity plan is developed or modified at the time the service is developed.
- **Recognizing that disaster can affect more than the bank's internal operations.** A community-based disaster can significantly impact the credit risk and borrowing demand of the bank serving the community. (For example, a bank providing bill payment services, although a small continuity risk from the bank's perspective, may have significant public relation issues if the bank does not pay its customers' bills on a timely basis.)
- **Leveraging continuity planning software.** Benefits to using this specialized software include:
  - facilitating distribution and availability of plan contents to authorized personnel; and
  - simplifying the maintenance and upkeep of the plan.

- Understanding the true cost benefits of continuity planning alternatives and having the courage to select the strategy that provides the greatest enterprise value. Unfortunately, there are no set rules, and cost-benefit and related strategies will vary significantly based on the individual bank's service and organizational politics. For example, a foreign branch located in the U.S. may decide that it is more cost effective to temporarily suspend trading activities or have head office perform trading activities than to have an elaborate continuity plan. Other banks choose to enhance their investment in one market segment (consumer access to cash) over another (for example, online 401(k) information).

### Conclusion

The biggest challenge faced by risk managers in planning for business continuity is the bank's ability to communicate and maintain the plan on a current and relevant basis. Although there is a lot of emphasis on policies and procedures to enforce this, at the end of the day, corporate culture plays a critical role in ensuring that everyone will be prepared. Many banks are challenged in accomplishing this. Elements of the following can help banks effectively derive the benefits of planning:

- Stress that continuity planning is people first—safety, family, and, in some cases, the ability of the business to provide for employees and the community.

- Market the need to maintain and periodically review the plan. Depending on the bank, the campaign can include such awareness items as mugs, calendars, or desk items.
- Send e-mail reminders on a periodic basis about the need to review the plan and share war stories or about how plans helped other organizations.
- Print wallet-size cards with key instructions for the users. Use positive reinforcement (for example, nominal cash spotter prizes or mention in internal memos that the selected employees had access to their contingency information).
- Provide peer pressure among the departments to update and maintain their plans, by publicizing (internally) departments that have successfully reviewed their plan or entering those departments into some type of reward promotion (for example, an evening of bowling).

At the end of the day, the best way to ensure the effectiveness of the continuity plan is to have employees recognize its importance and be personally motivated to maintain it. □

*Lanz invites you to visit*  
[www@itriskmgt.com](http://www@itriskmgt.com)

### Notes

<sup>1</sup> There are many documented examples of how banks and their personnel rose to the occasion to serve the public in this difficult time. An interview with Todd Gibbons of the Bank of New York appearing in the December 2001/January 2002 issue of *The RMA Journal* provides an outstanding example of both the heroics and preparation needed to successfully continue operations.

<sup>2</sup> 1996 FFIEC IS Examination Handbook, Chapter 10, page 1.