

AuditOne Advisory

From Bud Genovese, CEO

The Top Five Most Common Mistakes Made Implementing Business Continuity Plans

Last month we shared with you numbers 10 through 6 of the ten most common mistakes banks make when implementing Business Continuity Plans (BCP). Below, as promised, are the Top Five. Again, we've compiled this list through objective, independent internal auditing and testing and by comparing regulatory requirements with actual real world implementation data. I trust this list will be instructive as you prepare and update your bank's Business Continuity Plan. Here then are the top five most common BCP errors.

5. Both contingency and recovery are not considered for each function.

Contingency is the procedure taken when key resources (for example, Internet access) are not available. Recovery procedures are those procedures necessary to get the key resource back up and running. Each procedure should be managed by a different team.

4. Data communications is not considered.

Banks that outsource their core systems are heavily dependent upon their communications, yet many have no written contingency or recovery procedures should their connectivity go down. Provisioning new lines may take weeks without a procedure, and even days with a procedure. As a contingency, bank staff should know how to run the bank without reliable access to the Internet or core system.

3. BCP is missing a risk assessment.

This risk assessment evaluates the likelihood of various natural, technical, and malicious intent threats affecting bank data availability. The impact of reputation, operational, compliance and other risks posed by disasters must be considered. The Interagency guidance in "Lessons Learned from Katrina" states that any function that has a high impact to the institution when disrupted, despite how unlikely it may be, should receive additional emphasis in the planning process.

2. BCP is missing a Business Impact Analysis (BIA).

Regulators consider a BIA essential to a comprehensive BCP. The bank's first step in the BCP should be the development of the BIA. The BIA phase identifies the potential impact of uncontrolled, non-specific events on the institution's business processes, and determines what and how much is at risk by identifying critical business functions and prioritizing them. A BCP without a BIA is considered incomplete and is subject to criticism.

1. BCP focuses on just IT instead of the entire enterprise.

The FFIEC Business Continuity Planning Booklet recommends the development of an enterprise-wide business continuity plan with all business units and their interdependencies considered. Disasters such as Hurricane Katrina underscore the need to anticipate threats appropriately across all levels of the bank, not just from the perspective of recovering information technology.

Please feel free to give me a call to discuss your Business Continuity Planning or to explore any aspect of your internal audit and risk management program. AuditOne's success is predicated upon client satisfaction, and we are dedicated to going the extra mile to serve your internal audit needs. Thank you.

Bud Genovese is founder and CEO of AuditOne LLC, a San Jose, California-based internal audit firm that focuses only on banks and their service providers. Mr. Genovese pioneered the concept of providing comprehensive, affordable, independent internal audit services by gathering wide-ranging, world-class expertise within one firm. AuditOne now serves over 100 clients throughout the Western United States, and nationally. Contact Bud Genovese at 408-980-8099 or bud.genovese@audit-one.com