

# Business Continuity Planning: Old Concept, New Imperative in Financial Services



**Rodney Nelsestuen**

Research Director, Cross Industry  
August 2008

## Executive Summary

Business continuity is no longer just a matter of staying in business. Continuous high *performance* is now a standard expectation of the marketplace regardless of the natural, technical, or human failures that can beset a financial services institution (FSI). Meeting this expectation in a business continuity plan (BC plan) requires identifying strategic vulnerabilities and critical interdependencies. This is especially true today when global sourcing and interdependence extend a financial institution's business beyond the confines of its domestic operations. Multisourcing potentially affects all aspects of the business, including IT infrastructure, application services, business processes, and customer-facing products and services. Speed and performance are basics to business functionality, as is the role of security in this new epoch of global financial services. In the face of new products and services, alliances and partnerships, and business and social trends, BC plans have never been in as much need of comprehensive review. BC plans must be constantly upgraded to meet the growing mandate for continuous, real-time business performance while protecting corporate value from harm. Financial services institutions (FSIs) need renewed investments in business continuity planning (BCP) to address new aspects of business, including the following:

- *New channels.* Incorporate business continuity coverage of new and emerging channels such as mobile financial services, which will change the nature of financial services as they enter the mainstream over the next five years.
- *Social networking.* Take precautions in light of emerging consumer behaviors such as social networking, which increase the risk of loss for the customer and multiply the avenues for attack that can result in business interruption.
- *Alliances and partnerships.* Coordinate and practice continuity plans with business alliances and partners to protect customer access to nonproprietary services (on which the FSI is judged by its customers despite their being delivered by other parties).
- *Speed and performance.* Ensure that continuity plans address the business imperative for speed and performance so that mission-critical and time-sensitive functions are available not only without interruption but at continuous high levels of performance.
- *Internal threats.* Identify internal business threats such as rogue trading and employee fraud that could have deleterious effects ranging from reputation risk all the way to financial failure of the FSI.
- *Third-party providers.* Require all third-party service providers to have their BC plans dovetail with the FSI's own plans to ensure uniform, agreed-on standards of performance as well as alignment of the details and timing of recovery procedures.

---

TowerGroup Research is available on the Internet at [www.towergroup.com](http://www.towergroup.com)

© 2008 The Tower Group, Inc.

May not be reproduced by any means without express permission. All rights reserved.

TowerGroup is a wholly owned subsidiary of MasterCard Worldwide and operates as a separate business entity with complete editorial independence. MasterCard Worldwide is not responsible for and does not necessarily endorse any opinions, statements, or other content presented by TowerGroup.

## **History Repeating Itself: The Return of Apathy About BCP**

Business continuity planning (BCP) was long considered a necessary evil, a function that took time, money, and effort that could be spent more profitably in other ways. But in the past decade two events occurred that changed the attitude toward BCP: "Y2K" preparations for the date change at the new millennium, and the man-made tragedy of September 11, 2001.

Business continuity preparations for Y2K became a project of epic proportions as financial services institutions and other companies invested millions of dollars to update and test every facet of their technology operations. FSIs established disaster recovery (DR) and business continuity plans to anticipate every imaginable eventuality. Critics later decried the effort as overblown since no serious consequences resulted as the clock struck 12:01, January 1, 2000, but others point to that fact as proof that all the effort paid off.

Sadly, 9/11 tested not only DR and BC plans, but the will of a nation and the global financial system. It tragically demonstrated the importance of people when a disaster occurs. The subsequent upgrading of BC plans to encompass people, process, and technology was nothing short of stunning and for the first time ever, FSIs gained the attention of all stakeholders in the BCP process.

In both of these cases, the focus was on ensuring that the organization could stay in business and function for a period of time until normalcy returned. Security was sometimes sacrificed to the greater need of continuing to conduct business, which created yet new risks of information and system breach and financial losses should BC and DR plans be activated.

Now, several years after the two seminal events, business continuity and disaster recovery seem to have faded into the background once again in too many FSIs. Plans and scenario-mapping efforts are often not well executed, walk-throughs are poorly attended, and budgets funding continuity are often cut. The 2007 downturn in the global financial services industry is in part to blame for the reduced investment of time, money, and effort in BCP.

Curtailed investment threatens the effectiveness of BC plans. Not only does it degrade IT and physical assets, but it may result in personnel not knowing what to do, or even where to look for instruction, in times of crisis. The result is a heightened likelihood that an FSI may not recover from a business interruption quickly enough to sustain itself financially, or will at the least lose stature as a trusted provider in the eyes of the marketplace.

## **New Imperatives for Business Continuity Planning**

The return to apathy about BCP comes at a time when the velocity of business continues to accelerate, when financial services keep extending their global reach, and when the amount of money at risk is increasing rapidly. Meanwhile, new threats to business continuity have arisen through new business trends:

- New and untested delivery channels are entering the mainstream at the same time as changing norms that foster risky behavior with sensitive information around a socially networked globe. Together, the two elements — mobile channels and social networking — pose the risk of inadvertent loss of information as well as data

breach by would-be fraudsters. Besides financial loss from identity theft or direct monetary theft, security breaches cause a long-term degradation of an FSI's reputation that has the potential to cripple the institution's brand.

- Serious internal breaches and misconduct have resulted in billions of dollars in losses. The most infamous examples are the 1995 demise of the 233-year-old UK-based Barings Bank in the wake of over \$1 billion in losses in unauthorized futures contracts and accounting fraud at the hands of a rogue trader. In January 2008, trading losses of \$7 billion occurred at the French FSI Société Générale at the hands of another rogue trader. In the intervening 13 years, other incidents occurred that resulted in FSI failures or takeovers. Trading firms today admit they expect more such losses in the future.

Not only are such incidents failures of risk management, but they represent security breakdowns that enabled perpetrators to penetrate an FSI's defenses and overcome control systems. The possibility of purposeful wrongdoing by insiders is therefore as essential a consideration for risk management as are threats from outsiders, human error, natural disasters, and IT failure issues addressed in traditional BCP. Such risks can be ameliorated by interweaving strong security policies throughout operations and continuity plans and continuously enforcing them.

Regulatory scrutiny of BC plans has increased. The March 2008 update to the Federal Financial Institutions Examinations Council (FFIEC) IT examination booklet on Business Continuity Planning recommends that BCP focus "on the impact of various *threats* that could potentially disrupt operations rather than on specific *events*" [emphasis added].

Even rumors can have an impact on business continuity. A run on Northern Rock in the United Kingdom in September 2007 occurred when news of the bank's fiscal troubles leaked to the public. The bank management's response was not well planned or executed. The bank's failure due to faulty management of financial risk and reputation risk resulted in a takeover by the UK government. Meanwhile UK bank HBOS weathered rumors of financial trouble, allegedly started by stock traders seeking to create profit opportunities, because management was prepared to react to market jitters with a strong, well-thought-out response that averted a run on its deposit base. These two incidents demonstrate significant changes in the nature of protecting an FSI's business continuity.

Unlike sudden natural disaster or terrorist attack, business risks due to malfeasance in the financial services industry evolve, sometimes gradually, altering the requirements for business continuity planning. Competitiveness demands continuous performance of the business, not just recovery. This is as true for common interruptions of operations as for new channels, behaviors, threats, and as yet unimagined events. Maintaining high performance as risks emerge and mutate at an ever-faster pace demands swift and decisive action. An FSI must upgrade its business continuity capabilities to withstand degradation and outright failure of operations while finding new ways to protect the integrity and security of its data. Security must be sound but flexible to assure proper access while preventing unauthorized access.

BC planners need to engage the entire FSI in understanding the importance of business continuity for the institution overall and embracing BCP. Planners can enlist the support of people throughout the enterprise by demonstrating that BCP protects the part of the business that *they* are responsible for.

## Traditional Business Continuity Planning Is Still a Valid Foundation

Business continuity planning should be an ongoing process. Although fundamental BCP processes that evolved in the last decade are still valid today, BCP should remain a mission-critical issue for senior management and the board of directors of any FSI. Because business continuity plans are sometimes viewed as tedious to develop, test, and maintain, boards too often fail to fully enforce their own policies and fail to invest time, effort, and resources in BCP as an ongoing process. Exhibit 1 outlines key elements of traditional BCP processes recognized by both business and regulators.

### Exhibit 1



## Classical Business Continuity Planning (BCP): Cascading Responsibility, Cyclical Process



Exhibit 1

Source: Federal Financial Institutions Examination Council; TowerGroup

### The Four Pillars of BCP

BCP Plan Coverage should include the four pillars of BCP, as listed in the exhibit. The first pillar is *business impact analysis* (BIA), which ranks every business function, facet, product, and service, along with the people and roles necessary to deliver them, according to importance to the business. Using this prioritization, the second pillar — a *risk assessment* of each BIA area — is completed to identify potentially disruptive events and rank them by likelihood of occurrence. By understanding both the likelihood and potential impact of an interruption, an enterprise can develop the third pillar of BCP — *risk management* plans. These plans should include amelioration efforts and risk offsets. *Risk monitoring*, the final pillar of BCP includes BCP testing and subsequent adjustments to the business continuity plan.

Fundamental to effective BCP is knowing the nature and location of critical data throughout the organization and who should have access to that data. Sound security practices authenticate user identity to ensure that data is delivered only to the authorized users. They also enable alerts and problem escalation when a security incident occurs. Without understanding the “what” and “where” of critical data, the “why” and “how” of protecting that data is left incomplete, and thus critical data can more easily be compromised if the plan is activated.

Because speed and performance are essential for business success, BCP best practices recover the right data first. This prioritizing of risk amelioration efforts requires incorporating a classification system in the FSI's risk management protocol. Determining which business functions and associated information are most crucial is the first step in identifying mission-critical data. For example, although availability of funds in deposit accounts is an obvious priority, information within the deposits service varies in importance — at least in the customers' eyes.

A system for ranking data and information allows business continuity planners to put the data and information in the right context. Daily management reports are not as critical as, say, daily exception reports. Because exceptions affect account balances and may be a signal of fraud, reconciliations should be put ahead of other management reporting functions in prioritizing the following components of business operations:

- The technologies that support the key functions
- The human resources and skills needed to implement BC reconciliation operations if the usual staff is not available
- The functions to be established for operating under alternative business processes
- By using risk assessment, business impact analysis (BIA), and a risk rating system, the FSI can develop reliable backup plans to stay in business and enforce its security standards.

### ***Revisiting Plans for Natural Disasters***

Even traditional threats of long standing such as natural disasters must be revisited within continuity plans. As hurricanes Rita and Katrina demonstrated in 2005, the impact of large-scale disaster especially threatens the viability of regional FSIs. That is because much of FSIs' redundancy either is built within their own network of resources (with, for example, one location and IT service center serving as the backup for another) or resides at offsite BCP locations that are still within the physical footprint of the institution. Moreover, the geographic scope of the potential damage makes it difficult for FSI staff to focus on business recovery when their personal lives are also deeply affected.

More geographically diverse continuity operations coupled with managed services or other outsourced backup plans heightens the importance of security. This is especially true when an FSI gives new and unknown people access to sensitive customer and business information. In the case of insurance claims, the customers' need for claim payment is urgent at the same time that the risk of fraud to the company is increased. In the face of degraded or interrupted technology systems and controls, security practices must take into account policy terms using traditional internal physical controls to manage security and strive for efficient claims

settlement while protecting the company from fraud. Clearly, other business risks increase at the same time that business continuity is interrupted or degraded.

A sophisticated view of security in BC planning, then, includes both physical processes and backup technology needed both to safeguard information during business interruption and recovery and to ensure access to the information by authorized users when a BCP is activated.

### **Extending BCP and Security to New Channels**

The emergence and evolution of new delivery channels requires changing and updating business continuity plans. In the early years of online banking access for account inquiry, security and continuity plans often were no more complex than simply shutting down the site if something seemed amiss. Customers encountering a “down” Web site were neither surprised nor put out. They would simply call or stop in at a branch office. Today, of course, interruption of the online experience is not acceptable. Thus, BCP must be an ongoing process that evaluates the criticality of a channel or service as it evolves and changes throughout its life cycle. As a channel becomes more important to FSI customers, security can become more complex and thus a source of frustration to users.

#### **Online Channels**

Online channels demand stronger authentication both for inherent security reasons and to respond to regulatory requirements, especially two-factor authentication. This comes at a time when user experience is a key differentiating factor for many FSIs, and consumers and other users do not expect security to be an encumbrance. Continuity in this environment requires more sophisticated technologies but also an element of ease of use. Text messaging to send one-time passwords or to request other out-of-band authentication is a familiar tool to an emerging generation that uses simple texting on the one hand and spends time in rich online social networks on the other. To this market segment, user experience tied to stronger authentication aligns with normal interaction and lifestyle trends.

#### **Mobile Channels**

Anomalies tied to mobile application activity or service interruption are rapidly becoming a serious issue for BCP. Mobile devices are entering the market in growing number and sophistication with browser, mobile application, and Short Message Service (SMS) text service delivery. The user base is also growing. TowerGroup projects that the number of mobile banking customers will grow from 5.7 million in 2008 to more than 42 million by the end of 2012.

As mobile channels enable more, larger, and more diverse financial transactions, security of the users' personal information and identity becomes more important. Security must be in place to protect data and information from theft or corruption and to ensure delivery to the user. Besides functioning as credit and debit cards, mobile financial services are going beyond alerts and messaging by providing the ability to conduct trading and investing activity, file insurance claims, and perform other financial services transactions via mobile devices. Near-field communications (NFC) is being adopted as a mainstream mobile technology to enable noncontact (or swipeless) payment. All of these factors open additional data vulnerabilities in real time and at the transaction level and show how much the marketplace values speed and performance. Once again, the growing number, speed, and immediacy of transactions puts financial information, and money itself, at risk.

### **Traditional Business Operations**

The importance of continuity planning in more traditional business operations has not diminished. The following examples demonstrate the need not just for disaster recovery but business continuity plans that provide continuous performance in more traditional settings.

- Any disruption affecting a bank's branch offices or disruption that prevents insurance policyholders from accessing claims assistance affects customer satisfaction. A positive experience is increasingly crucial to retention of customers and organic growth. Achieving organic growth requires selling more products and services per customer and attracting new customers through viral marketing in a more socially networked world.
- Corruption of trading system data — whether internal or through business partners or outsourcers — not only impacts investment decisions but also can result in huge losses occurring at a high rate of speed. Such events may go undetected for too long and impact financial results, and in some cases, the viability of an FSI.

### **Partnerships and Alliances**

The need for BCP coordination with business partnerships and alliances is increasing. FSIs' business continuity plans need to ensure the continuity and security of operations of their business partners or outsourcing providers while keeping operations seamless and running smoothly from the customer's perspective.

Financial and personal information and transactions must be protected in a more distributed environment. Coordinated business continuity plans therefore require sound security approaches that are aligned between the FSI and its business partners and service providers. Without strong alignment, the threat of a security breach and loss of information increases at points of hand-off between technology protocols, business processes, and people. Exhibit 2 (on the next page) suggests how this new environment must be coordinated with new and emerging business realities.

## **The BCP Cycle of Risk Management**

In today's business environment, the BCP process is more dynamic and demanding than ever before. Boards and management still hold the key to policy and plan quality, as has always been the case. Management must consider not only the operational areas that are crucial in disaster recovery but also the controls, security standards, and personnel training needed to maintain a dynamic yet effective business continuity plan.

The four pillars of BCP that were listed in Exhibit 1 — business impact analysis, risk assessment, risk management, and risk monitoring and testing — are shown in Exhibit 2 as a virtuous cycle of risk management.

**Exhibit 2**



**Dynamic Business Continuity Planning (BCP):  
A Virtuous Cycle of Risk Management**



Exhibit 2  
Source: TowerGroup

This cycle combines traditional elements of BCP such as risk weighting with response to new demands for speed of execution and heightened awareness of changes in the internal and external environment. More frequent updating and testing is necessary today, along with greater transparency and visibility into the risk environment. Applying this cycle continuously to update priorities turns BCP from an add-on or afterthought into a fundamental operational need.

**Best Practices in BCP**

It's obvious that today's BCP must respond to the dynamic nature of business while protecting against degradation of operations and breach of trust in any sense. In light of the increasing need for and value of data, both ongoing monitoring of business and IT and understanding how the two are aligned must be part and parcel of the business continuity plan. The best practices for BCP listed on the next page contribute to an even better goal: avoiding having to trigger implementation of a business continuity plan in the first place.

- Infrastructure monitoring serves as an early warning system for potential technological failure and highlights network and hardware attacks. It enables an FSI to respond to threats by adjusting security protocols and processes *before* a business interruption occurs.
- Business service management (BSM) is increasingly popular to monitor the junction between infrastructure and business using function-based prioritization of IT. Well-executed ongoing BSM informs business continuity plans by identifying and maintaining critical IT and business assets.
- Data discovery tools are increasingly important because the proliferation of data in multiple locations makes it hard to manage multiple instances and duplication of data. One cannot protect what one does not know about.
- Master data management (MDM) initiatives rationalize and deduplicate data under a disciplined set of data definitions designed under a well-governed data architecture. MDM makes security approaches more effective overall by imposing standards with regard to type, structure, definitions, and locations of data.
- Secure remote authentication for employees is essential. It enables employees to log in to critical systems securely when and if they need to work in remote locations in the aftermath of a disaster.
- Authentication methods also require balancing risk with user satisfaction. The adoption of mobile financial services and the spread of social networking have heightened the importance of customer training and education regarding protecting their personal identification information. Protecting the ongoing operation of an FSI tomorrow thus requires that users become an active part of the solution.
- Finally, security incident and event management (SIEM) disciplines are most effective when a comprehensive security program covers both normal operations and those in effect in the event that an organization's business continuity plan is triggered. SIEM makes it possible to easily audit the efficacy of security practices and fosters evaluations that identify weaknesses and gaps across the FSI. It is in no small part the quality of security practices that can reduce the risk of having to activate the business continuity plan in the first place.

In sum, these best practices contribute to the best business continuity plan — the one that is never needed!

## Conclusions

Business continuity planning must be viewed as a part of the ongoing operations of an FSI, not just an afterthought. The need to update traditional BCP disciplines is critical to an FSI's becoming more dynamic and vigilant in protecting its reputation in the marketplace in addition to ensuring the performance of the company continues in times of disruption. To that end, BCP cannot be a function that resides separately in an FSI with only a dedicated team of people responsible for it. Such an approach results in a continuity plan that is always playing catch up to the business.

In today's dynamic and high-velocity business environment, time lost when business fails to function as designed means money lost. That said, boards of directors and senior managers hold the key to the quality and outcomes of BCP, and everyone in the institution as well as its suppliers, outsourcers, business partners, and even customers have a stake in current business activities and functions that either contribute to or detract from the effectiveness of both the business continuity planning process and its outcome when triggered by disruptive events.

Finally, business continuity planning must be viewed as a critical business and IT activity that is an ongoing and dynamic process. Failing to improve business continuity capability is in essence failing to secure the FSI's information and data, access to that information by employees, customers, and partners, and the processes and technologies that assure the viability of the institution itself.



*RSA, The Security Division of EMC, commissioned TowerGroup to conduct independent research and analysis of business continuity practices and trends in financial services. The content of this report is the product of TowerGroup and is based on independent, unbiased research not tied to any vendor product or solution. Although every effort has been taken to verify the accuracy of this information, neither TowerGroup nor the sponsor of this report can accept any responsibility or liability for reliance by any person on this research or any of the information, opinions, or conclusions set out in the report.*