



# Planning *Outlook*

for the Financial Industry:

Analysis and Recommendations  
on Trends and International  
Guidelines for Business Continuity

## Letter from the President

The unique aspect of financial services industry is that money in all its forms—or perhaps more accurately, information about money—is the industry’s only product. And technology provides the value chain, rather than enhancing or enabling it. In a very real way, computers and networks are the factory *and* the warehouse *and* the distribution channel in many cases. Financial companies have historically been on the forefront of innovation with regard to IT continuity and recovery.

Now, almost two years after the events of September 11, 2001 which tested the industry’s reliance on technology and shook it to its very core, international consortiums, government agencies, and industry taskforces are drafting new guidelines designed to secure the world economy through continuous information availability and rapid restoration of key operations.

The need to keep this information chain connected—both within and across organizations—is today’s top priority. We increasingly hear the term “resilience” used in the financial services industry to characterize this relationship. At SunGard Planning Solutions (SPS), we start with the premise that it is the business process that we must make resilient by addressing the role of technology.

While this may seem obvious, we mention it because we see the need for this industry to embrace the conception of prevention, not just recovery. For critical functions, the financial services industry must think of building resilience into the business processes and the supporting technology. Disaster recovery and business continuity have not become less important. However, organizations must incorporate proactive design into their production environment to deliver the resilience that today’s guidelines and regulations—and indeed the board and consumers—are requiring.

As the leading provider of planning software and services, SPS is on the forefront of issues impacting continuity and availability. In this paper, we take a broad look at the new body of government regulations and agency recommendations that have been released to address business continuity planning and operational resilience. We review emerging trends and their impact on your organization. And we present our recommendations for meeting these guidelines and incorporating information availability and operational resilience throughout your organization. We hope this paper will provide valuable background on the regulatory climate in the financial services industry and help your organization build a more resilient organization.

Sincerely,



Kenneth A. Smith  
President, SunGard Planning Solutions



## TABLE OF CONTENTS

Executive Summary . . . . .	1
Operational Resilience and the Role of Technology . . . . .	2
Trend Analysis. . . . .	5
Recommendations . . . . .	13
Conclusion. . . . .	17
About SunGard Planning Solutions . . . . .	19

## Executive Summary

In the wake of the September 11th attacks and three years into an intransigent bear market, the robustness of the financial services industry remains under heightened scrutiny. Forced to reconsider the role of technology in their organizations, executives must determine how to ensure its resilience, viability, and availability. New questions must be asked and answered about business continuity and operational resilience. Now the board is seeking to understand *how* the organization is protected, not just *if* it is protected. And a new model is emerging that considers the “process interface,” “collective interdependencies,” and the pervasive technology infrastructure that interconnects the vast financial community value chain.

Recent regulatory publications and recommendations have stimulated the industry to acknowledge that information technology (IT) is now a critical part of operational risk—along with people and processes—that were traditionally outside the purview of risk management. These landmark guidelines require proactive measures, based upon the immediacy and depth of a specific firm’s potential impact.

In this paper, SunGard offers insight into trends that affect how the financial industry addresses information availability, business continuity (BC), and operational resilience. We offer recommendations on ways to integrate these concepts into your current business processes while evolving to a more risk-aware and risk-averse organization. Finally, we offer a brief overview of the significant guidelines and regulations impacting the market and accelerating the move to operational resilience.

## Operational Resilience and the Role of Technology

*Technology ... is a queer thing. It brings you great gifts with one hand, and it stabs you in the back with the other.* C. P. Snow, 1971

It is doubtful that C. P. Snow could have realized how prophetic that statement would become. At the time, his quote marked the beginnings of a technology revolution. Now, it stands as testament to the double-edged sword of IT. The financial industry constantly exploits technology for cost savings and improved transaction time. However, the business benefits gained from the technology are at the expense of creating some of the largest risks in your organization.

Technology is the engine driving today's financial services business model. Only recently—due in part to 9/11—has the industry begun to recognize that technology is indeed ubiquitous, its protection is paramount, and the impact of any failure extends far beyond the confines of any single financial organization.

And while technology is certainly the engine, information is the fuel that drives the financial world. Given the current economic climate and slim profit margins, business managers are investing heavily in technology to achieve greater efficiency from operations. In this drive for improved profitability, automation and integration have increased to the point where business is completely dependent on technology to maintain the flow of information.

The lessons learned from 9/11 are well known—the holes in BC planning, telecommunications issues, and the oversight of the “human” factor. In a larger sense, however, 9/11 was a vivid reminder of the



potentially devastating systemic impact of a widespread incident. With so many external dependencies in the financial services sector, that day truly challenged the resilience of the financial industry and heightened the ripple effect of such an event outside the institutions directly affected.

Unprecedented steps were taken on 9/11 and thereafter to prevent the potentially devastating impacts on the global economy. With US stock and bond markets closed as a result, it was imperative that investors around the world know that the world's largest economy hadn't been paralyzed. At 11:45 am, only *three* hours after the attacks began, Federal Reserve Vice Chairman Roger Ferguson announced “The Federal Reserve system is open and operating ... [and] available to meet liquidity needs.” The Fed, and other key regulatory authorities, took additional bold steps in the hours and days after 9/11 to ensure that there was minimal market impact of the events. (See sidebars for additional information.) While a catastrophe was averted, Ferguson later acknowledged, “It is increasingly clear that the operational resilience of the largest financial institutions in key markets needs to reflect their systemic impact across the financial sector.”<sup>1</sup>

---

<sup>1</sup> Ferguson, Roger W., Jr., Vice Chairman, Board of Governors of the Federal Reserve. Speech given at the Conference on Bank Structure and Competition. May 9, 2002.

## The Fed Enables a Systemic “Soft Landing”

On 9/11, the US financial system was under great stress. “It was clear that the loss of so many key resources at the core of the financial capital of the United States would strain markets,” Federal Reserve Vice Chairman Ferguson noted. “If allowed to mount, those strains could prompt a chain reaction drying up liquidity, which, unchecked, could lead to real economic activity seizing-up. The shocks to the financial system and the economy that were possible could have been disastrous to the confidence of businesses and households in our country and, to a significant degree, the rest of the world.” If banks were to run out of US currency, “international commerce, international trade, international finance would also have been at risk and potentially have slowed and ground to a halt,” he continued.

To avoid a potential crisis, Ferguson infused the US financial system with record amounts of cash. The Federal Reserve usually lends US banks about \$100 million each day to ensure smooth operations; on September 12, the Fed lent \$45 billion. Typically, the Fed exchanges no foreign currency into dollars; on September 12 and 13, it exchanged \$90 billion worth. Additionally, the Fed arranged for the availability of reciprocal currency facilities of up to \$50 billion with the European Central Bank and \$30 billion with the Bank of England, both in the form of 30-day swaps, and lifted the ceiling of a pre-existing swap with the Bank of Canada to \$10 billion.<sup>2</sup>

While discussion of “operational resilience” remains at the forefront of the financial industry’s agenda, “resilience,” “risk” and “impact” are not new terms for the financial services industry. However, the deeper meanings of risk and resilience have been evolving beyond traditional concepts and definitions as the relationship between fundamental business processes and technology has grown increasingly interdependent.

Federal Reserve Governor Susan S. Bies notes that “enterprise-wide risk management has been evolving as financial theory has advanced, new technology has made modeling of risks more feasible, and innovation has helped to find better ways to mitigate risk.” Bies identifies three broad categories for risk—market, credit, and operating.

“Market risk arguably has evolved the furthest because of the transparency of markets, frequency of transactions, and financial engineering that can parse the various forms of risk exposure so that appropriate financial instruments can be developed to hedge the specific components of risk.” Credit risk has likewise become more quantifiable with use of models that analyze “a corporate customer's or borrower’s probability of default, the loss in the case of default, and the borrower’s likely exposure at the time of default, taking into consideration future draw-downs.” But, Bies importantly notes that “operating risk is the least developed, as conceptual frameworks, metrics, and databases are still in preliminary stages.”<sup>3</sup>

---

<sup>2</sup> *Ibid.*

<sup>3</sup> Bies, Susan S., Federal Reserve Governor. Corporate Governance and Risk Management. Speech given at the Annual International Symposium on Derivatives and Risk Management, Fordham University School of Law, New York, New York, October 8, 2002.

## The Numbers Behind 9/11

In addition to the Federal Reserve, other key regulatory authorities and financial service providers acted swiftly in response to the events of 9/11. The Securities and Exchange Commission (SEC) adopted a number of temporary rules to prevent stocks from crashing when the markets reopened and used its power to grant exemptions for selected market participants from certain provisions of both the Securities Exchange Act of 1934 and the Investment Company Act of 1940. Another set of exemptions allowed the American Exchange to operate while hosted by the New York Stock Exchange (NYSE).<sup>4</sup>

The Depository Trust & Clearing Corporation (DTCC)—the world’s largest post-trade infrastructure organization—had billions of dollars in trades outstanding from the previous three days. DTCC quickly contacted its network of settling banks and the Federal Reserve to reconfirm its ability to make and receive payments. Most of the firms affected by 9/11 were supported by their banks through the first settlement cycle. By 9/12, DTCC had settled nearly \$300 billion in trades. Out of a daily average of roughly \$110 billion in commercial paper, the DTCC had to recycle nearly \$45 billion for later settlement.<sup>5</sup>

“Operational risk” was used as early as 1988 in the first Basel Capital Accord—where it was defined as the ability to reduce and prevent disruptions to business processes.<sup>6</sup> Today, the proposed new Basel Capital Accord (Basel II) and other guidelines are extending the definition to include technology directly—that is, to impose stringent protections for any failure in the technology infrastructure.<sup>7</sup> Striking the proper balance between operational risk, technology dependence, and the cost of business continuity has increased in importance since 9/11. The combination of high dependence on IT and tightly-integrated processes leaves financial services organizations at great risk. And, the cost of ensuring the highest levels of availability and complying with multiple guidelines requires organizations to carefully weigh their options.

The financial industry is under internal and external pressure to mitigate systemic risks, recognize interdependencies, and establish sound practices with stated recovery and resumption objectives. The historically reactive discipline of BC has been stretched beyond its comfortable boundaries. IT departments, business leaders, executive managers, and regulatory bodies are now being forced to rethink continuity in terms of resilience and availability—and the impact on the business of an organization, as well as the national and global financial infrastructure.

---

<sup>4</sup> SEC Notice: Order Under Sections 6(c), 17(d), and 38(a) of the Investment Company Act of 1940 Granting Exemptions from Certain Provisions of the Act and Certain Rules Thereunder, release no. 25156, September 14, 2001.

<sup>5</sup> Considine, Jill, Chairman and CEO. The Depository Trust & Clearing Corporation. Market Risk: Old Calculations, New Perceptions. Speech given at the Bond Market Association’s Credit and Risk Management Conference, October 16, 2001.

<sup>6</sup> Basel Committee on Banking Supervision. Basel Committee Publications No. 4 (Basel Capital Accord). July, 1988.

<sup>7</sup> Basel Committee on Banking Supervision. New Basel Capital Accord (proposed). January, 2001.

## Trend Analysis

Determining the levels of information availability and resilience that your organization requires is not a simple task. The requirements within the financial industry simply extend beyond the standard business imperatives that other industries face—demand for product, customer satisfaction issues, stock performance, etc. And, these same pressures are compounded by a broader set of rules, regulations and risks that affect the underpinnings of the global economy.

These risks, combined with the current regulatory climate, create challenging and expanding trends that must be examined as part of your resilience planning. The implications of the following trends are key to the financial industry.

### 1) Regulations will stiffen as government agencies endeavor to reduce economic risk.

In late 2002, the landmark *Draft interagency white paper on sound practices to strengthen the resilience of the U.S. Financial System* (Draft paper) was published.<sup>9</sup> While similar guidelines and recommendations have existed on the international front, this Draft paper clearly served as the harbinger for such recommendations throughout the US financial services industry. By April 2003, the Final paper was issued, further refining recommendations and clarifying points from the comment period.<sup>10</sup> In addition, a broad range of organizations, including the NASD, the US SIA, the NYSE, the FFIEC, the FSA, and the MAS released their own

## Systemic and Enterprise Risks

Systemic risks: "Risk that the failure of one institution in the financial system to meet its required obligations will cause other institutions to be unable to meet their obligations when due, thereby potentially causing significant liquidity dislocations or credit problems and threatening the stability of the financial markets."<sup>8</sup>

- Increased interdependence
- Faster transaction cycles and straight-through processing (STP)
- Regulatory issues
- Ubiquity of operations
- Globalization
- Consolidation
- Conglomeration
- Global threats

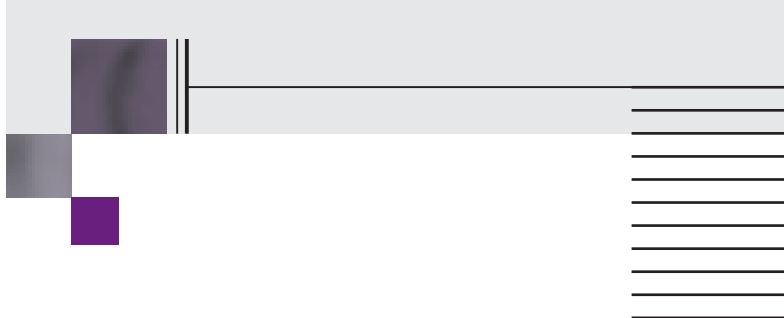
Enterprise risks: Risks that the infrastructure (people, processes and technology) dependencies within any given financial institution will affect its ability to meet customer and fiduciary obligations, impacting initially the stability of the individual enterprise with secondary impact upon partners and the industry.

- Dependence on third-party providers
- Exposure to physical attacks
- Broadening scope of continuity requirements
- Cyber security concerns
- Exposure from wireless applications
- Dependence on telecommunications
- Human capital concerns
- Centralization vs. decentralization

<sup>8</sup> The Monetary Authority of Singapore. *Guidelines on Business Continuity Planning*. January 10, 2003.

<sup>9</sup> The Board of Governors of the Federal Reserve System, the Office of the Comptroller of the Currency, the Securities and Exchange Commission, the New York State Banking Department, and the Federal Reserve Bank of New York. *Draft interagency white paper on sound practices to strengthen the resilience of the U.S. Financial System*. September 5, 2002.

<sup>10</sup> *Ibid.*



recommendations/guidelines, making a complicated situation even more challenging. (As this issue went to press, the FFIEC issued its new auditors' handbook focused on business continuity.)

Even self-regulated bodies, such as the NASD, will require more robust continuity strategies. And, the effect of this increased scrutiny on BC will extend beyond just the biggest banks and brokers into the

requirements, and satisfying fiduciary responsibilities is a considerable task.

Additionally, the financial industry also faces compliance issues outside the “operational risk” focus—such as the extensive anti-money-laundering rules established in the US Patriot Act of October 2001. According to recent research,<sup>12</sup> US banks and insurance and securities companies will spend

**Predictions for Key Trends**

- 1) Regulations will stiffen as government agencies endeavor to reduce economic risk.
- 2) Robust continuity and resilience plans will be essential to creating investor confidence and will prove to be a competitive advantage.
- 3) Reliance on technology will continue to grow at a record clip as straight-through processing (STP) galvanizes the market, forcing organizations to acknowledge the risk that technology poses to their organization.
- 4) The drive to adaptive engineering—infrastructure and technology to ensure information availability—will supplant simple disaster recovery solutions.
- 5) A stronger focus on partners up and down the value chain will emerge, with the growing requirement for integrated testing.
- 6) Consolidation and conglomeration efforts will begin to address issues of risk and resilience.
- 7) Geographic dispersal will gain favor as a business continuity strategy.
- 8) Globalization forces organizations to rethink continuity and resilience.

entire financial services marketplace. In a recent presentation, Alfred R. Berkeley III, Vice Chairman of the Nasdaq Stock Market, Inc., commented that one of the driving goals of the National Association of Securities Dealers Automated Quotation (NASDAQ) was to “make the engine of capitalism efficient and effective.”<sup>11</sup> Accomplishing this goal, meeting new “operational risk”

\$11 billion by the end of 2005 to comply with these regulations. Beyond the need for further IT investments to meet these requirements, the growing set of regulations forces internal competition for technology dollars and increases the dependence on the reliability and availability of the infrastructure.

---

<sup>11</sup> Berkeley , Alfred R., III, Vice Chairman of the Nasdaq Stock Market. Speech given at Titans of Technology Luncheon, Eastern Technology Council, Malvern, PA, February 24, 2003.  
<sup>12</sup> Cuneo, Eileen Colkin. Beyond Compliance. *Information Week*, February 24, 2003: 20-22.



***2) Robust continuity and resilience plans will be essential to creating investor confidence and will prove to be a competitive advantage.***

Business continuity is steadily migrating from the IT center to the boardroom. In a recent global study,<sup>13</sup> nearly 34 percent of respondents indicated that BC was a board-level post (C-level). Protecting shareholder value and increasing revenue remains at the forefront of every corporate initiative and requires companies to continue to build their brand. However, building a brand is based largely upon trust and instilling customer, partner, and employee confidence. Business continuity planning and a focus on operational resilience contribute directly to building confidence—from board members to investors to consumers.

Further, assuring investors of the resilience of the organization will become increasingly valuable in competitive situations, as organizations compete for both customers and partnerships. As business continuity requires board-level review, the marketplace will look for outside verification of BC plans, much like Gramm-Leach-Bliley<sup>14</sup> compliance certification. Organizations must ensure that

technology has not opened new doors of risk and vulnerability. We believe those organizations that have made continuity and resilience a corporate imperative will be able to leverage that mindset with customers, partners, and investors.

To ensure that the risk posed by technology has been considered in the business process, we see a growing integration of tasks and budgets. Organizational priorities and application criticalities most certainly affect operational resilience. Budgets and plans for disaster preparedness and BC should be integrated with technology production budgets to move more swiftly toward a resilient model.

Every organization is seeking to leverage their IT investments as they address conflicting budgetary priorities (for example, compliance vs. funding for the Patriot Act initiatives). Some are trying to fund capital projects for dedicated recovery solutions that encompass fully redundant data centers and workspace to “guarantee” recovery. Other organizations are turning to detailed analysis and solution design to match the criticality of specific applications with a more cost-effective mix of commercial shared and dedicated solutions.

In short, we see a trend toward organizations balancing the spending across technology, business processes, and people—and budget lines being redrawn to reflect that intra-organizational task. Ultimately, the problem is “to balance the efficiency of the solutions with the opportunity costs and the change of expectations on the side of clients and regulators.”<sup>15</sup>

<sup>13</sup> Is Responsibility for Business Continuity Moving Higher Up the ‘Chain of Command.’ *Globalcontinuity.com*, March 24, 2003.

<sup>14</sup> S. 900, The Financial Services Modernization Act of 1999 (Gramm-Leach-Bliley Act of 1999). November 4, 1999.

<sup>15</sup> Francotte, Pierre, Chief Executive Officer, Euroclear Bank. Cantor-Fitzgerald, Verizon, and metropolitan risks. In *Resilience and Value: financial institutions creating value in a post-9.11 world*. Paris, France. PROMETHEE, 2002: 46-53.

*3) Reliance on technology will continue to grow at a record clip as straight-through processing (STP) galvanizes the market, forcing organizations to mitigate the risk that technology poses to their organization.*

With the rise in expectations from technology and its capabilities, the financial services industry is being pressured from the outside and from within to deliver tighter tolerance in many back-end processes, including clearing, settling and funds transfer. For example, increased trading volumes and associated settlement risks are driving the move to STP in securities processing. Other areas of the marketplace already have aggressive clearing in place. Government bonds are T+1 while cash trades, options trades, and repo trades are all T+0. As cycle time is removed from the market, the risk from any single point of failure also increases.

The challenge of STP and increased integration (on both the buy side and sell side) will have a downstream market impact as it is adopted, much like supply chain management has affected even the smallest trading partners. Further, the intra-day or next-day recovery and resumption requirements outlined in recent regulatory guidelines will further drive the process integration. Compressing time and eliminating manual processes through technology enables greater throughput, but drastically reduces the recovery timeframe and the flexibility to adapt.

*4) The drive to adaptive engineering—infrastructure and technology to ensure information availability—will supplant simple disaster recovery solutions.*

We see a new paradigm where the intelligence gleaned from years of disaster preparedness is leveraged proactively into process, application, and organizational design. While the need for traditional DR remains, it can be synthesized into

day-to-day processes, ensuring a more resilient infrastructure. Rather than ex post facto efforts that are disjointed and costly, future success requires building availability and resilience at the front end of your IT infrastructure and business processes.

In fact, while the Final paper details the requirements for wholesale clearing and settling, it also reinforces this thinking by outlining three BC objectives for all financial firms:

- Rapidly recover and resume critical operations after a wide-scale regional disruption.
- Rapidly recover and resume critical operations for loss of staff in at least one major operating location.
- Perform robust testing for internal and external continuity arrangements.

Marketplace confusion is forcing technologists to evaluate the resilience and recoverability of *any* infrastructure and recovery strategy. Existing clustering technologies, while providing a layer of redundancy and production resilience and touted as disaster recovery solutions, are not business continuity solutions when deployed in close

proximity. Government agencies prefer to see distance-based strategies and their guidelines have proposed solutions for intra-day and next-day recovery that pose significant technology challenges. However, as new solutions overcome existing technology barriers (60-mile synchronous limits, for example), architectures must be re-engineered for flexibility and adaptability. Current business models and guidelines dictate that information availability be considered at the front end of any technology decision.

***5) A stronger focus on partners up and down the value chain will emerge, with the growing requirement for integrated testing.***

The SWIFT-PROMETHEE Report, *Resilience and Value, financial institutions creating value in the post-9.11 world* states, “Financial institutions, even more than other organizations, know the importance of cooperative assets and tied assets. Their value-creation processes rely on market infrastructures that are either cooperatively developed or heavily regulated, and on immaterial ‘goods’ like market liquidity that are co-produced with others. Every single institution has to be considered as one element within the financial ‘network of networks’, itself a key ingredient in the global networked economy.”<sup>16</sup>

As an industry, the financial sector has always had to balance interdependencies, competitions and regulation. Today’s marketplace is shrinking in the number of key players, yet expanding in the touch points inside and outside the organization. Financial service organizations have become increasingly reliant on a smaller number of companies (through consolidation, clearing exchanges, specialist service providers, and other niche operators). As a result, external dependencies

have become concentrated, leading to the real threat of a massive domino effect if any member of the chain were to fail. The “resilience” of any given interdependency is only as strong as its weakest link.

Based on the current state of regulatory papers, we look for an increase in more rigorous testing. Since it is imperative that continuity arrangements of critical market players be effective and compatible with others in their sector, this will require the development of common testing metrics to improve the ability to survive an outage. Enhancing the testing process will accomplish the following:

- Confirm the ability of chosen recovery strategies to match business objectives.
- Identify vulnerabilities and exposures so they can be remedied.
- Address ongoing change in the organization’s infrastructure.
- Identify dependencies on other organizations.

***6) Consolidation and conglomeration efforts will begin to address issues of risk and resilience.***

Business continuity and operational resilience issues are increasingly drawing the attention of executive management and the board. As this “awareness” becomes further ingrained, it will help them recognize that decisions made in the boardroom for business reasons directly impact operational resilience. For every action, there is an equal and opposite reaction.

One example is consolidation activities in the financial sector. There were just under 1,000 thrifts, with total assets of \$960 billion in June 2002 versus 1,952 thrifts in 1992 with assets of \$839 billion. Similarly, the number of insured commercial banks decreased from approximately 11,450 in 1992 to about 7,960 as of June 2002.<sup>17</sup>

<sup>16</sup> PROMETHEE. *Resilience and Value: financial institutions creating value in the post-9.11 world*. Paris, France. 2002.

In Europe, particularly since the introduction of the Euro in 1999, emerging patterns of cooperation and consolidation have grown among central counterparty clearing houses (CCPs). Several CCPs exist and mergers/alliances are increasing. A central counterparty clearing would affect “the smooth execution of monetary policy operations, the smooth operation of payment and settlement systems and the stability of the financial markets in general. The consolidation process adds to the complexity of the issue: on the one hand, consolidation in central counterparty clearing could help to increase efficiency in the clearing and settlement of securities; on the other hand, the potential systemic consequences of a central counterparty’s failure increase with its size.”<sup>18</sup>

At the management level, the “risks” assessed during a consolidation process have typically focused more on credit and liquidity risks. However, consolidation within any industry removes layers of redundancy and increases overall systemic risk. As noted by Vice Chairman Ferguson, “having diversified forms of risk intermediation makes the financial system more robust. In this instance, having markets and banks that performed similar financial intermediation roles accounted for much of our financial system’s ability to withstand the shock of September 11.”<sup>19</sup>

Conglomeration produces a similar vulnerability. Gramm-Leach-Bliley removed the traditional barriers between financial institutions, enabling a single corporate entity to provide banking,

securities, and insurance products. However, expansion of services by financial institutions exposes new areas of compliance and testing, particularly with the abundance of marketing partnerships that have been created to provide single-point-of-service for customers.

“Consolidation and the pursuit of competitive positioning will continue ... with companies merging or being acquired across borders and across time zones.”<sup>20</sup>

#### *7) Geographic dispersal will gain favor as a business continuity strategy.*

One of the greatest lessons learned from 9/11 was the need for less “concentrated risk” both within an organization and in the overall financial marketplace. These dispersal strategies must include consideration of the infrastructure and the human element. 9/11 revealed the devastating impact—far beyond resumption of business process—of the loss of human life. Even as technology reduces the vestiges of human intervention, access to intellectual capital factors directly into an organization’s operational resilience. From basic emergency planning information to details about sophisticated trading processes, far too much information was locked in the minds of a few people. In fact, the recent General Accounting Office (GAO) Report on Potential Terrorist Attacks, the GAO states that of the 15 key financial market organizations that perform trading and clearing functions reviewed, nine had not developed BC planning (BCP) procedures “to ensure that staff capable of conducting their critical operations would be available if an attack incapacitated

---

<sup>17</sup> Olson, Mark, W., Federal Reserve Governor. The Banking Industry in 2002 after a Decade of Change. Speech before the First Annual Convention of the Ohio Bankers League, Columbus, Ohio, November 12, 2002.

<sup>18</sup> The European Central Bank. *The Eurosystem’s Policy Line with Regard to Consolidation in Central Counterparty Clearing*. September 27, 2001.

<sup>19</sup> Ferguson, Roger W., Jr., Vice Chairman, Board of Governors of the Federal Reserve. September 11, the Federal Reserve, and the Financial System. Speech at Vanderbilt University, Nashville, TN, February 5, 2003.

<sup>20</sup> Considine, Jill, Chairman and CEO, The Depository Trust & Clearing Corporation. Market Risk: Old Calculations, New Perceptions. Speech given at the Bond Market Association’s Credit and Risk Management Conference, October 16, 2001.



personnel at their primary sites. Ten were also at greater risk for being disrupted by wide-scale events because four organizations had no backup facilities and six had facilities located between two to ten miles from their primary sites.”<sup>21</sup>

In addition to issues of recoverability, organizations must strike a balance between cost savings derived from central locations and consolidation against the mitigated risk obtained through geographic dispersal. 9/11 drove organizations to question how far a secondary recovery site, secondary operations, and tape backups need to be from the primary site. That day, Verizon and AT&T reported heavy damage to five major telecommunications switching stations and a substantial amount of commercial networking equipment, including the destruction of 36 miles of communications cabling and 300,000 telephone lines. Con Ed lost two major electrical substations and also reported the

loss of 33 miles of electrical cable.<sup>22</sup> While the NYSE was technically fully operational, it did not reopen until Monday, September 17 when voice and data links were restored. As a result, organizations are adding telecommunications redundancy to their planning efforts and evaluating the benefits and costs of such alternative technologies as wireless, Internet, and satellite communications.

However, while geographic dispersal does mitigate the impact of a regional disaster and of the “concentrated risk,” it does not fully address how to minimize the impact of an event on the collective interdependence of the financial industry. Firms must consider the need for separate power grids, separate telecommunications carriers, and separate transportation providers as part of their resilience strategy. And they also must seriously consider human capital dispersion strategies to protect their intellectual capital.

<sup>21</sup> United States General Accounting Office. *Potential Terrorist Attacks: Additional Actions Needed to Better Prepare Critical Financial Market Participants*. Report to the Committee on Financial Services, House of Representatives, February, 2003.

<sup>22</sup> DRI•WEFA. *Financial Impact of the World Trade Center Attack*. Prepared for the New York State Senate Finance Committee, January 2002.

8) *Globalization will force organizations to rethink continuity and resilience.*

“Now the system [clearing and settlement] is so international that there needs to be a global answer to design a global solution.”<sup>23</sup> Technology *has* erased borders, particularly in the financial services industry. With the increased dependence on capital flows for liquidity of operations in global markets, there is more dependency on international infrastructure. The trend toward increased globalization means massive amounts of data must be treated and accessible across international borders—and in almost real time. While this was already particularly difficult for multi-national institutions, recent guidelines and regulations make it challenging to determine which regulations take precedence and how to comply.

Globalization presents large risks, particularly since instability in one country or area can adversely affect other countries. This is currently being addressed by the establishment of an overall market discipline. Despite the prevalence of national and international guidelines, however, financial institutions are still individually challenged to set internal policies to minimize the immediate impact of global events. In her speech at the Bond Market Association’s Credit and Risk Management Conference in October 2001, Jill Considine,

Chairman and CEO of DTCC said, “Throughout that whole week [9/11], some of the most critical work in our company took place overseas. As you know, Cantor Fitzgerald had to piece their operations together through their London offices. For the first time, market executives in London found themselves clearing and settling trades in the U.S. system. This was a novel experience for them ... We taught an overnight course in continuous net settlement.”<sup>24</sup>

While the world prepares for the possibility of more physical attacks on wealth and power, equally threatening are attacks on the technology infrastructure of the world economy. As a distributed architecture yields more points of failure but disperses risk, so does a distributed, yet tightly interdependent, financial infrastructure. Experiences, such as the one described above, will likely increase in frequency, forcing organizations to consider the role of global operations into any recovery plan.

---

<sup>23</sup> Large, Sir Andrew, Deputy Chairman of Barclays plc and Chairman of the Project on Global Clearance and Settlement for the “Group of Thirty,” In *Resilience and Value: financial institutions creating value in a post-9.11 world*. Paris, France. PROMETHEE, 2002: 160-164.

<sup>24</sup> Considine, Jill, Chairman and CEO, The Depository Trust & Clearing Corporation. Market Risk: Old Calculations, New Perceptions. Speech given at the Bond Market Association’s Credit and Risk Management Conference, October 16, 2001.

## Recommendations

Resilience can be defined as “the capacity to protect value creation against major discontinuities and stress-losses through risk mitigation processes, adjustments, and constant learning.”<sup>25</sup> In the largest sense, resilience is the ability of an organization to assess the potential impact of market forces (such as the trends previously discussed) and build an enterprise infrastructure that considers the entire realm of risk posed by human and physical attributes, internal and business processes, and technology and information architectures. The emphasis on risk and the need for building resilience was clearly accelerated by 9/11. However, it is apparent that other technology-forward initiatives, such as STP, would have driven the industry to elevate the ideas of continuity into a broader discussion of the resilience of the business model.

The trends we outlined earlier, combined with the acknowledged systemic risk to the market and potential damage to national and international financial/economic infrastructures of any disruption, have compelled many regulatory and financial authorities to publish new guidelines for BC. In the sections below, we present our recommendations for meeting these guidelines and beginning to incorporate information availability and operational resilience throughout your organization. Discussion points from the industry guidelines are included, with a summary of some major guidelines presented in the Appendix for further review.

***1. Recognize that your selected level of information availability becomes a service level agreement (SLA) in your supply chain and can be leveraged as a competitive advantage.***

A highly resilient infrastructure leads to competitive advantage. Organizations will make choices that either further this goal or hinder their competitiveness.

### RATIONALE

Your organization has an existing level of availability—whether is explicitly defined or selected by default. It is a combination of your recovery time objective (RTO) and your recovery point objective (RPO), plus a layer of production resilience. RTO is the amount of time that has elapsed from the point at which a disruption has occurred until the specified business operation is resumed and current business transactions can be applied. RPO measures the amount of potential data loss in number of hours from the time of interruption. Current regulations and recommendations have clearly begun defining the level of availability for key industry segments and raise the bar to new levels.

The Final paper recommends standards for “recovery” and “resumption” that are more strict than previous regulations and advisory standards. Wholesale clearing and settling firms must meet aggressive RTOs, which will drive planning and testing activities that should be consistent across critical markets. The RTO is defined as two hours for “core clearing and settlement” organizations to “recover and resume” within the business day in which the disruption occurs. The RTO for “significant players” within the wholesale market is 4 hours for recovery within the business day. This requirement for intra-day recovery and resumption drives the need for high information availability and operational resilience in order to capture “same-day” transactions (RPO) and meet RTO objectives.

---

<sup>25</sup> PROMETHEE. *Resilience and Value: financial institutions creating value in the post-9.11 world*. Paris, France. 2002.

Similarly, in the GAO report cited earlier, that office calls on regulators (specifically the SEC) to develop “complete strategies” that identify where trading could be resumed or which organizations must conduct trading if a major exchange or multiple broker-dealers were inoperable for a prolonged period. The SEC disagreed with that suggestion, stating that the focus on clearing organizations in the Final paper addressed a critical function that

even if not for the financial “utility” providers? What is the business value of BC and resilience? One case in point: within three days following the 9/11 attack, S&P cited DTCC performance under the pressure of the crisis and reaffirmed its triple A credit rating for the depository and clearing corporation subsidiaries.<sup>27</sup> Success is rewarded, as is preparedness.

**Recommendations**

- 1) Recognize that your selected level of information availability becomes a service level agreement (SLA) in your supply chain and can be leveraged as a competitive advantage.
- 2) Find the proper balance between the degree of risk your organization is willing to assume and costs associated with mitigating it.
- 3) Establish a process to determine which level of resilience is required for each of your business processes

was performed by a few institutions, whereas trading could be performed by many. Broker-dealers are required to ensure completed trades are cleared and settled, and that customers gain access to their accounts “as soon as physically possible.” These firms are not required to conduct trading or provide liquidity to markets. Therefore, it was proposed that it should be a “business decision” for these firms to develop their business continuity programs.<sup>26</sup>

Is resilience a “business decision,” a “business imperative,” or a process worthy of mandating,

Earlier, we spoke of the complex interdependencies in the financial sectors as the “value chain.” To minimize the impact of any “internal” weak link in this value chain, BCP has long emphasized the importance of testing. As the move to operational resilience gains momentum, we are witnessing growing understanding in the business continuity world that testing means more than the internal IT infrastructure. Rather, it includes validating the business recovery process and production availability plans throughout the organization and across the value chain.

<sup>26</sup> Colby, Robert L., Deputy Director, Division of Market Regulation, U.S. Securities and Exchange Commission. Recovery and Renewal: Protecting the Capital Markets Against Terrorism Post 9/11. Testimony before the House Subcommittee on Capital Markets, Insurance, and Government-Sponsored Enterprises, Committee on Financial Services, February 12, 2003.

<sup>27</sup> Considine, Jill, Chairman and CEO, The Depository Trust & Clearing Corporation. Market Risk: Old Calculations, New Perceptions. Speech given at the Bond Market Association’s Credit and Risk Management Conference, October 16, 2001.



Many of the new guidelines/recommendations reinforce this approach and specifically require external integrated testing in addition to internal testing. The Draft paper offered specific directives for testing: “conduct joint tests with partner institutions” and “conduct cross-organizational tests to assure the compatibility of individual recovery and resumption strategies within and across critical markets.” The Final paper requires that firms routinely use or test recovery and resumption arrangements and explore broader industry stress test options. This testing must include connectivity and capacity, as well as major counterparties and third-party service providers, and should demonstrate an ability to achieve the prescribed RTO.

An integrated testing scenario is a requirement to ensure industry resilience; however, the logistics of such testing are daunting. Drawing a comparison to another event that required enormous industry cooperation, Ferguson commented, “Obviously, in preparing for Y2K we engaged in very large-scale testing. In the current context we understand that there may ultimately be diminishing returns from repeated testing and that we must learn from our experiences in preparing for Y2K. The industry again is working together to help define reasonable and meaningful tests and to cooperate by participating in them.”<sup>28</sup>

Can resilience then be leveraged as a competitive advantage? The answer is yes. Having a business continuity plan in place and ensuring thorough testing helps to ensure enterprise recoverability—and is a strong testament to the board, management, customers, and employees. As noted by Leonard H. Schrank, CEO of SWIFT, “I believe it’s possible to quantify resilience. It captures the savings from not losing business because you’re down, or late. It’s the extra business you earn if your customers have the confidence that you will always deliver, around the clock and around the world. It’s peace of mind.”<sup>29</sup>

<sup>28</sup> Ferguson, Roger W., Jr., Vice Chairman, Board of Governors of the Federal Reserve. Business Continuity after 11 September. Presented at the SWIFT Closing Plenary Session, October 3, 2002.

<sup>29</sup> Schrank, Leonard H., CEO, SWIFT. CEO’s address. Presented at the SWIFT Plenary Session, October 1, 2002.

**2. Find the proper balance between the degree of risk your organization is willing to assume and costs associated with mitigating it.**

To choose the correct strategy for true operational resilience, organizations must assess what is reasonable risk in light of their fiduciary responsibility to their clients and counterparts in the economic infrastructure. Effective continuity planning has always balanced the cost of a solution with the degree of risk that a company is willing to assume. The lower the risk and the tighter the time constraints, the more expensive the strategy becomes.

**RATIONALE:**

“Who decides when there are enough ‘9s’ in 99.99999%? If Basel II were to come up with an answer, it would be very nice. Trying to reach perfection has a high cost!”<sup>30</sup>

Choosing an infrastructure design without a clear understanding of its limitations does not support the goal of operational resilience. Each technology decision has its own set of unique benefits and associated risks. Quantifying these risks is emerging as another necessity for the new model of BCP. Indeed, concepts of resilience and availability will soon be considered as part of business return on investment (ROI).

In the original Basel Capital Accord (1988), the G-10 central banks addressed the issue of credit risk by agreeing to apply common minimum capital standards to their banking industries. Implemented



in 1992, the Accord is monitored by the Bank for International Settlements (BIS–Basel, Switzerland). In response to a new set of exposures to the banking community that was not covered in the original accord, the BIS issued the New Basel Capital Accord (commonly referred to as Basel II) in January 2001.

Under Basel II, larger institutions will have to apply, at a minimum, the Foundation Internal Ratings Based Approach for credit and the Standardized Approach for operational risk. Basel defines the effective management of operational risk as “the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events”—a much broader definition of operational risk than previously adopted by the market. For the smaller institutions, one key player noted, “by transforming the best practices of the best-managed banks into rules for others, we hope to give the right incentive to banks to move up the ladder of sophistication.”<sup>31</sup>

<sup>30</sup> Ludvigsen, Joel, Head of Customer Value, SWIFT. The SWIFT infrastructure and the post 9.11 backup architectures. In *Resilience and Value: financial institutions creating value in a post-9.11 world*. Paris, France. PROMETHEE, 2002: 147.

<sup>31</sup> Nouy, Daniele, Secretary General, the Basel Committee on Banking Supervision, Bank for International Settlements (BIS). The new Basle Accord, a Foundation for sustainable value creation. In *Resilience and Value: financial institutions creating value in a post-9.11 world*. Paris, France. PROMETHEE, 2002: 134-139.

Specifically, Basel II proposes an operational risk charge that could amount to 20% of total capital. For those institutions that implement the recommended approaches to credit and operational risk, there are possible financial incentives and a potential lower charge. However, organizations must undertake significant work to get processes for gathering credit and operational risk data in line, and, where relevant, to develop appropriate models.

Additionally, the recent GAO report notes that “organizations are having difficulty determining how to best invest their resources to mitigate risk. On the one hand, measures need to be implemented to protect facilities and systems; on the other hand, these resources could be best spent expanding business continuity capabilities.”<sup>32</sup> These considerations force organizations to rank the value of information availability and resilience to ensure that expenditures are appropriate and reasonable. In short, operational resilience and continuity planning “boil down to the problem of accurate assessment of need. The critical mistake to make in resourcing is to overspend in certain areas while underspending in others; a chain is only as strong as its weakest link.”<sup>33</sup>

### *3. Establish a process to determine which level of resilience is required for each of your business processes.*


A resilient enterprise starts with a robust, cohesive strategy. Organizations need to create this strategy by prioritizing business processes that *cannot* fail, identifying people, processes, and technology to support that process, and determining acceptable RTO and RPO for less critical business processes.

#### RATIONALE

Financial organizations were among the first to elevate business continuity planning beyond the data center. While the recent flurry of regulatory activity has increased the attention on BC, the financial services industry has consistently been at the forefront of that industry. However, as business continuity and production availability goals continue to converge, organizations need to adopt a line-of-business (LOB) planning strategy. By looking at their technology in terms of business process and applications, rather than systems and networks, the actual business requirements and interdependencies become clear. By conducting this dependency mapping, organizations make informed decisions about technology, LOB, and enterprise priorities.

<sup>32</sup> United States General Accounting Office. *Potential Terrorist Attacks: Additional Actions Needed to Better Prepare Critical Financial Market Participants*. Report to the Committee on Financial Services, House of Representatives, Washington, DC: February, 2003.

<sup>33</sup> Datamonitor. *Business Continuity in Financial Services*. London, England: January, 2003.



Organizations can start this challenging task by looking at the applications that support the business model. It is critical to analyze the applications, the systems that support them, the business processes they power, and the impact of their inaccessibility. To strike the balance between cost effectiveness and recoverability, we suggest analyzing the applications according to a tiered technology plan. Applications can commonly be divided into different tiers of mission-criticality and recovery staging order, based on recovery technology requirements. A core financial institution's applications might be prioritized in this manner:

- Tier 1 applications are the most mission-critical and require an RTO of 0 to 2 hours and an RPO of zero data loss. They typically include funds transfer, online banking, trading, and ATM applications.
- Tier 2 applications require an RTO of less than 24 hours and have an acceptable RPO ranging from zero data loss to less than 2 hours. They typically include advisory services, reporting, e-mail functions, and call center software.
- Tier 3 applications have an RTO of greater than 24 hours and a typical RPO of 24 to 32 hours. They usually include administrative applications, such as payroll, general ledger, and development or R & D efforts.

Successful risk-based planning dictates that an organization define the level of availability required for each tier, identify the business processes that rely on the application, and weigh that against how much it can afford to spend to achieve the desired availability.

Inherent in this process is the challenge of separating the data and systems according to tiers and then maintaining that separation. The complexity of application and data interdependence—and the fact that some applications may be regulated and others not—further complicates this process. Should organizations invest their time separating the applications internally to protect the regulated applications differently than other applications? Or should they spend more time to protect a great percentage of their data and business? By creating a strategy that prioritizes your business processes and desired levels of availability, you will be able to determine the best answer to those questions for your organization.

## Conclusion

“Operational risk differs from credit risk or market risk in the sense that, unlike credit risk, no one willingly takes it on as part of an investment strategy.”<sup>34</sup> While this risk may not be taken on voluntarily, operational risk affects the underpinnings of any financial institution’s investment strategy. Basel acknowledges this viewpoint by directing organizations to consider how technology choices affect the amount of capital that needs to be set aside for resilience. This concept of “set aside” will continue to permeate the industry.

As a result, continuity and resilience issues across and beyond the organizations will continue to receive high-level management involvement. Executives are increasingly forced to demonstrate good corporate governance. Business continuity and operational resilience directly affect corporate governance and ultimately, the bottom line. As a leader of your organization, you need to ask questions about how your organization has prioritized business processes and allocated budgets. What technology strategies are in place to assure your production availability and minimize your operational risk? How is this important task being addressed across the enterprise? Has your organization accepted that technology infrastructure risk will increasingly become part of determining operational risks?

Whether your organization is one of the institutions directly impacted by the Final paper, or a smaller institution that operates regionally, the themes of these regulations will impact you. Any company that hasn’t done so should set up a board-level review process to evaluate resilience of critical processes in light of changing needs and technology. Issues raised in these new recommendations and regulations—such as testing dependencies, accessibility and redundancy, and risk management—will continue to dominate industry discussion and future regulatory guidance.

While there is no easy answer, we hope that this paper has provided you with the background on the regulations and the emerging trends. SunGard Planning Solutions has helped thousands of customers balance the requirement for operational resilience and business continuity against the realities of budgets and timelines. To learn more about how SunGard can help you, contact us at 800.434.0002 for more information, or visit our website at [www.planning.sungard.com](http://www.planning.sungard.com).

---

<sup>34</sup> Nouy, Daniele, Secretary General, the Basel Committee on Banking Supervision, Bank for International Settlements (BIS). The new Basle Accord, a Foundation for sustainable value creation. In *Resilience and Value: financial institutions creating value in a post-9.11 world*. Paris, France. PROMETHEE, 2002: 134-139.

## About SunGard Planning Solutions

SunGard Planning Solutions delivers specialized business continuity and operational risk assessment services to all segments of the financial industry—from the operator of the Northeast’s largest electronic funds transfer system to the nation’s oldest stock exchange.

SunGard Planning Solutions’ comprehensive services help organizations assess risks, build information security and business continuity plans and programs, and continually test and improve them. Services include:

- Risk Management Services, including Information Security Risk Assessment and Facility Risk Assessment
- Disaster Recovery and Business Continuity Planning, including Business Impact Analysis, IT Recovery Planning, and Incident Management Planning
- Professional Services, including Continuity Program Management and Testing Service
- Technology Infrastructure services, including Application Impact Analysis, Recovery Strategy Options Analysis, High Availability Options Analysis, and Network Design and Analysis

SunGard Planning Solutions, SunGard eSourcing, and SunGard Recovery Services form the **SunGard Availability Services** group. Together, the companies deliver a full continuum of capabilities, including information security and business continuity consulting services and production- and recovery-oriented availability solutions. **SunGard eSourcing** delivers managed hosting, security, and outsourcing services, providing the ultimate in security, reliability, and value. **SunGard Recovery Services** provides both dedicated and shared continuity solutions, including end-user recovery, mobile recovery, and high availability solutions.

SunGard Availability Services is a operating group of **SunGard (NYSE:SDS)**, a global leader in integrated software and processing solutions for financial services. SunGard serves more than 20,000 customers in over 50 countries, including 47 of the world’s 50 largest financial services companies. SunGard is a member of the S&P 500 and has annual revenues of more than \$2 billion.

◀ **Open here for an overview of the new government regulations and agency recommendations that have been released to address business continuity planning and operational resilience.**

## General Description

## Main Points

## SPS Commentary

### Basel Capital Accord New Basel Capital Accord

**Key dates**  
7/88, first issue;  
1/01, second issue.

**Originator(s)/authors**  
The Basel Committee on Banking Supervision

**Targets/audience**  
National and international banking industry regulatory bodies.

Comments on the amount of capital that firms must keep on reserve to cover operational, market, and credit risk.

Recommends statements of best practice in the expectation that individual national authorities will take steps to implement them through detailed arrangements. Expected to align with EU Capital Review Third Capital Adequacy Directive (CAD3).

Due to the interconnected nature of the financial services industry and since 9/11, Basel's focus on and definition of operational risk is gaining greater influence and attention.

While Basel's main thrust remains traditional liquidity measures, writings from industry pundits indicate recognition of risk posed by technology dependence and a move toward inclusion of technology infrastructure in operational risk and business continuity.

We are seeing more national agency and multinational companies acknowledge that operational risks for systems include information security and business continuity planning.

### Interagency Paper on Sound Practices to Strengthen the Resilience of the US Financial System

**Key dates**  
4/7/03 issued. "Core" compliance EOY 2004, "Significant" firms by 2006.

**Originator(s)/authors**  
The Board of Governors of the Federal Reserve System, the Office of the Comptroller of the Currency (OCC), the Securities and Exchange Commission (SEC), and the Federal Reserve Bank of New York

**Targets/audience**  
For sound practices, wholesale clearing and settling (not trading or retail):

- Core clearing and settlement organizations—market utilities and private sector firms with significant aggregate market share who would cause systemic risk in the event of their failure.
- Firms with "significant" roles in critical financial markets—those who clear or settle at least 5% of value of transactions in that market.

For business continuity objectives, "all financial firms."

The paper identifies sound practices aimed at minimizing the immediate systemic effects of a wide-scale disruption on critical financial markets. The paper also identifies three new business continuity objectives that have special importance for all financial firms post September 11.

Outlines 4 sound practices for critical settlement and clearing organizations:

- Identify critical clearing and settling back-office activities and the systems that support them in order to ensure process recovery.
- Determine the appropriate recovery time objective (RTO), which will drive planning and testing activities and should be consistent across critical markets. (The RTO is defined as two hours for "core clearing and settlement" organizations to "recover and resume" within the business day in which the disruption occurs. The RTO for "significant players" within the wholesale market is 4 hours to recover within the business day.)
- Maintain sufficient geographically-dispersed resources (staff, equipment, and data) to meet recovery objectives.
- Routinely use or test recovery and resumption arrangements and explore broader industry stress test options. (Testing must include connectivity and capacity, as well as major counterparties and third-party service providers, and should demonstrate an ability to achieve the prescribed RTO.)

Outlines 3 business continuity objectives for financial firms:

- Rapidly recover and resume critical operations after a wide-scale regional disruption.
- Rapidly recover and resume critical operations for loss of staff in at least one major operating location.
- Perform robust testing for internal and external continuity arrangements.

The draft white paper emphasized the criticality of protecting the financial system from serious new risks posed in the post-September 11 environment and described a set of sound practices that were identified by industry participants during a series of interviews and meetings with the agencies. After reviewing the approximately 90 comment letters and continuing their dialogue with interested persons, the agencies issued a revised final interagency paper. The paper formally recognizes and addresses interdependency within the financial market and requires BC objectives for all financial firms.

The sound practices identified therein are intended to supplement the agencies' respective policies and other guidance on BCP for financial institutions. However, they focus only on establishing robust back-up facilities for those back-office activities necessary to recover clearance and settlement activities for the wholesale financial system in times of serious disruption. Therefore, they do not address issues relating to trading operations or to retail financial services.

While it indicates no hard-and-fast mileage requirements, the paper does stress significant distance and separate labor pools for core firms. It also addresses the need for backup transportation, telecom, and electricity, among other things. And, it specifically states that "core" firms should have backup a "significant distance away" from their primary sites. This commentary will ultimately drive changes in the way firms develop employee operations and opens the door for greater emphasis on true telecommunications diversity. More importantly, the paper is a good indicator that the agencies will continue to push for more and better geographic diversity as technology improves.

It is important to note that testing received heavy emphasis in both sections. For example, the paper states that firms should be able to demonstrate their ability to achieve two-hour or four-hour RTOs through testing. This emphasis is a good indication that testing and its objectives will see greater regulatory attention and there will be increased emphasis on showing improvement in results from one test to another. Auditors will specifically examine Board of Directors' commitment.

## NASD Rule 3500 3510 3520

### Key dates

3/02, issued; 8/7/02, filed with the SEC as a proposed rule change; 9/9/02, notice filed with the Federal Register.

### Originator(s)/authors

National Associations of Securities Dealers' (NASD)

### Targets/audience

Member organizations—securities firms that do business with US consumers (more than 5,600 organizations.) NASD is self-regulated with varying size in membership firms.

This document outlines rules that would enhance business continuity planning in member companies.

Would require members to create and maintain business continuity plans:

- At minimum, address:
  - Data back-up and recovery (hard copy and electronic)
  - Recovery strategies for mission-critical systems
  - Financial and operational assessments
  - Alternate communications between customers and the institution
  - Alternate communications between the institution and employees
  - Business constituent, bank, and counter-party impact
  - Regulatory reporting
  - Communications
- Conduct an annual review and update of the BC plan and examine the need for change(s) in light of operations, structure, business, or location
- Make plans available for inspection by NASD staff
- Voluntarily submit plans to a central repository service
- Keep current and file emergency, reviewing twice annually, contact information with the NASD, such as senior management, key banking relationships, and clearance and settlement information

The overriding goal of this document is to ensure investor protection and market integrity in the event of a business disruption. This enhanced scrutiny resulted from record-keeping scandals and a general lack of 9/11 business continuity planning preparedness. While most will avoid having to meet federal requirements, compliance will be driven by other members in the value chain.

## SIA Business Continuity Planning Committee Best Practices Guidelines

### Key dates

8/5/02, issued; immediate compliance.

### Originator(s)/authors

US Securities Industry Association's (SIA) Business Continuity Planning Committee

### Targets/audience

Member organizations—broker dealers, exchanges, electronic communications networks (ECNs), industry utilities, service bureaus, and market data vendors (more than 600 securities firms.)

This document provides overview recommendations for member firms' business continuity programs and plans.

Guidelines for member firms' BC program and recovery strategies and resources:

- Develop, implement, test, and maintain BC and emergency response plans that enable organizations to protect assets and meet recovery objectives
- Prevent and mitigate the impact of a disruption
- Institute an ongoing employee awareness program
- Develop recovery strategies that enable organizations to continue critical operating, service, and technology functions
- Ensure the availability of resources required to meet recovery objectives
- Recommends annual reviews and updates.
- Dictates executive oversight for planning and testing.

This document highlights service level agreements (SLAs) between partners and underscores the need for geographic dispersment of recovery strategies. The SIA was an active participant in post-9/11 hearings. These guidelines support a stronger push for executive oversight. Additionally, the SIA concurs with the GAO report and agrees that trading is also important to industry resilience and should comply with the regulations.

## Securities Industry Association Business Continuity Planning Committee Plan for Industry Testing, Version 1

### Key dates

9/10/02, issued; testing began 9/02.

### Originator(s)/authors

US Securities Industry Association's (SIA) Industry Testing Workgroup

### Targets/audience

Member organizations—broker dealers, exchanges, electronic communications networks (ECNs), industry utilities, service bureaus, and market data vendors (more than 600 securities firms.)

This document seeks to ensure that major institutions, exchanges, and industry utilities can simultaneously activate work area and data center recovery plans from alternate sites.

Looks to confirm that financial institutions can activate work area and data center recovery:

- Use a two-phased approach that is focused on the back-up and alternate recovery sites
  - Test communications from back-up or alternate sites to primary sites of critical parties
  - Test a specific geographic area for a disruption to supporting infrastructure

Several SIA members will be covered under the "systematic risk" provision of the final Interagency paper, which will drive more stringent continuity requirements for the industry as a whole. These guidelines demonstrate the increased emphasis in SIA on business process recovery, in addition to technology recovery. The plan emphasizes successful and improved testing. This emphasis will trickle down the value chain.

## FSA Working Paper on Business Continuity Management

### Key dates

5/02 issued.

### Originator(s)/authors

UK Financial Services Authority (FSA)

### Targets/audience

UK financial industry

Not a formal consultation paper, this document captures the FSA's "current thinking" on the BCM process within the context of events on the scale of those of 9/11.

Includes a matrix that highlights key aspects of BCM that firms should consider in developing strategies and the risks that arise from these issues:

- Examine organizational concerns and responsibilities
- Assess threats and perform business impact analysis (BIA)
- Institute a crisis management plan
- Ensure timely business resumption
- Assess IT and telecom systems
- Assess general, workspace recovery, and IT recovery outsourcing
- Develop alternative BCM strategies

Although advisory in nature, this document offers more specific mention of crisis management planning than in any current US advice or regulations. As such, firms should consider adopting the guidelines, regardless of geography. The major goal of the FSA is to maintain market confidence through prudent management of operational risk. Citations that reference BCP as part of good internal controls include SYSC 3.2.19G and PRAG 6. The document highlights the need for executive accountability. The FSA's major concern is flexibility so as not to impact smaller firms too severely.

**Consultation Paper 142--  
Financial Services Authority  
Operational risk systems and  
controls consultation paper**

**Key dates**

7/02, issued; compliance scheduled for sometime in 2004—after the final policy is published.

**Originator(s)/authors**

UK Financial Services Authority (FSA)

**Targets/audience**

UK financial industry

This guidance is intended to help firms reduce the frequency and impact of operational risk management failures in a cost-effective way that furthers statutory objectives.

Seeks to mitigate operational risk as defined by the Basel Committee (“the risk of loss, resulting from inadequate or failed internal processes, people, and systems, or from external events”) and is aimed at ensuring a firm can continue to function and meet its regulatory obligations in the event of an unforeseen interruption:

- Assess the various internal and external events that may disrupt operations
- Plan for responses to possible disruptions
- Organize appropriate back-up site arrangements
- Evaluate outsourcing relationships for BC, DR, and other functions

Although advisory in nature, this paper is indicative of the emerging importance of the Basel Accord’s definition of operational risk. FSA presentations have stressed concepts of SLAs within the industry. Increased emphasis on recovery of business processes. FSA is clearly aligning with Basel and CAD3, as well as Risk Management Framework inherent in the Stock Exchange Combined Code D2.1 (Turnbull).

**A risk-focused Review of  
Business Continuity Manage-  
ment in Major Financial Groups  
Post September 11, 2001**

**Key dates**

9/12/02, issued.

**Originator(s)/authors**

UK Financial Services Authority (FSA)

**Targets/audience**

UK financial industry

This document provides review results of 12 major financial groups to identify examples of good practice. This “is not a formal consultation paper and does not represent formal guidance.”

Advises financial services institutions “with the main purpose of establishing the preparedness of firms for major disruption”:

- Prepare for disruption on a scale not previously envisioned
- Make BCM a board-level issue and encourage group responsibility
- Align approaches to crisis management, business continuity, and disaster recovery
- Perform rigorous tests that gauge the effectiveness of the plan, measure the assumptions on which they are based, and identify any key weaknesses with third-party providers
- Re-examine third-party relationships

Although advisory in nature, this paper highlights the UK financial firms’ lack of preparedness in addressing a major disruption to the industry. It also reflects the Basel definition of operational risk.

Note: FSA has issued only consultative advice on system risk and the need for business continuity planning. However, HM Treasury has also solicited comments on the prospect of introducing additional legislation, refer to CM5751, The Financial System and Major Operational Disruption, February 2003.

**Notice of Filing of Proposed Rule Change  
by the New York Stock Exchange, Inc.  
Relating to Business Continuity and  
Contingency Planning, New Rule 446**

**Key dates**

9/9/02, issued. Federal Register, Vol. 67, #174.

**Originator(s)/authors**

New York Stock Exchange (NYSE)

**Targets/audience**

Members and member organizations of the NYSE (more than 2,800 listing companies) acting in concert with the National Association of Securities Dealers (NASD.)

The proposed rule would require members and member organizations to develop, maintain, review, and update business continuity and contingency plans for an emergency or significant business disruption.

Aims to minimize the impact future disruptions will have on the securities industry:

- Develop and maintain a written business continuity and contingency plan
- Make the plan available to the Exchange upon request
- Conduct a yearly review of the plan for changes in operations, structure, business, or location.
- Include at (at minimum) the following in the plan:
  - Books and records back-up and recovery (hard copy and electronic)
  - Identification of all mission-critical systems and back-up for such systems
  - Financial and operational risk assessments
  - Alternate communications between customers and the firm
  - Alternate communications between the firm and its employees
  - Alternate physical location of employees
  - Business constituent, bank, and counterparty impact
  - Regulatory reporting
  - Communications with regulators
  - A senior officer, identified to the Exchange, who is responsible for the plan and annual review and the official emergency contact

Defines “mission-critical system” as any system “that is necessary to ensure prompt and accurate processing of securities transactions, including order taking, entry, execution, comparison, allocation, clearance, and settlement of securities transactions, the maintenance of customer accounts, access to customer accounts, and the delivery of funds and securities.”

This rule change was written in direct response to the events of 9/11 and aimed at ensuring that members can continue their business in the event of future significant disruptions. The guidelines expressly define financial and operational risk and align closely with similar NASD filings. The rule places strong emphasis on business recovery, rather than just system recovery.

**MAS Consultation Paper—  
Guidelines on Business  
Continuity Planning**

**Key dates**

1/10/03 issued; 2/10/03 comment period expired

**Originator(s)/authors**

The Monetary Authority of Singapore (MAS)

**Targets/audience**

Financial sector participants

The paper encourages the adoption of BC practices by financial institutions in Singapore to strengthen their resilience against widespread disruptions.

Proposes and discusses the following seven principles:

- Board and management should take responsibility for the BCP preparedness of their institution.
- Institutions should embed BCP into their business-as-usual operations, incorporating sound BCP practices.
- Institutions should test their BCP regularly, completely, and meaningfully.
- Institutions should develop recovery strategies and set recovery time objectives for critical business functions.
- Institutions should understand and appropriately mitigate interdependency risks of critical business functions.
- Institutions should plan for wide area (zonal) disruptions.
- Institutions should practice separation policy to mitigate concentration risk.

The paper acknowledges that the events of September 11 “highlighted vulnerabilities that may not have been fully appreciated before, such as the concentration of staff, processes, and technology.” The paper addresses these issues, as well as their significant interdependencies, via seven principles that cover resilience, recovery, and risk management. Detailed and well-conceived, the guidelines make a strong call for executive management. The forward-thinking paper recommends incorporating business continuity planning into change management and on-going business decision making.

**SUNGARD<sup>®</sup>**  

---

**PLANNING SOLUTIONS**

680 East Swedesford Road  
Wayne, PA 19087  
484-582-2000  
800-434-0002  
610-687-5130 Fax  
[www.planning.sungard.com](http://www.planning.sungard.com)