

SunGard
Availability Services
Outlook Series

Outlook



*The Convergence of
Risk and Regulation*

*The Information Infrastructure
and Its Impact on Corporate
Governance*

Letter from the Group Chief Executive Officer

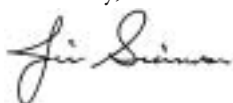
We are experiencing a convergence of the elevated need for reliability, privacy and accountability brought about by significant events in the last decade. World commerce and information technology are profoundly and permanently interconnected. Data security and privacy concerns are pervasive, and threats have expanded to include situations that are both intentional in nature and difficult to quantify and anticipate.

Because they have a vested interest in maintaining financial stability and investor confidence, government agencies are taking no chances when it comes to ensuring appropriate business continuity, disaster recovery and information security measures within private industry. Although the mandates themselves usually only address an individual area within the broader discipline of production availability, they are all rooted in the desire to ensure the continuation of the world economy. That's why SunGard believes this myriad of regulatory demands converging on companies is best served by an overarching program that takes a holistic approach to corporate governance.

As the leading provider of information availability, continuity and recovery services, SunGard is on the forefront of integrating the various facets of resiliency into an IT infrastructure. In this paper, we examine those areas and provide a framework for taking a more comprehensive approach to corporate governance as it relates to information management, security and availability. We also review regulatory trends and highlight underlying similarities among rules for emergency preparedness, operational resilience, internal control and production availability.

We hope this paper provides valuable insight to this often confusing—and increasingly difficult—area and helps your organization build an information availability program that reflects best practices in regulatory compliance.

Sincerely,



Jim Simmons

Group Chief Executive Officer, SunGard Availability Services

The Evolution to Maximum Exposure—Steady and Sure

The heightened level of concern and scrutiny we are seeing from government agencies did not happen overnight. Rather, it has been progressive and consistent, building slowly but steadily. And, while there may be disagreement regarding the specific genesis of this current regulatory climate—some mark it at Year 2000 initiatives and others view the earlier 1993 World Trade Center attacks as the watershed moment—all agree that it shows no signs of abating.

There is also consensus regarding the general motivation. That is, a universal governmental desire to ensure the continuation of a services-based world economy by mandating an ideal level of preparedness within industries and individual organizations.

Our dependence on technology has grown such that technology disruption has become one of the requisite components when calculating operational risk. But the underlying truth is, regulators react to threat and the perception of threat.

Market Crash 1929

The stock market crash of 1929 resulted in the passage of an array of laws regulating financial and commercial activities and culminated in the establishment of the SEC. This increased regulatory scrutiny was designed to ensure the reliability of US banking and trading systems in the wake of the country's worst economic depression. And as the way we do business has evolved, so have the regulatory requirements. When we automated those systems in the 1970s, government and industry evolved their thinking to involve technology reliability and continuity.

Year 2000

The Year 2000 "scare" was the first widespread event that demonstrated how application- and technology-driven our economic infrastructure had become. In February 1998, the President established The President's Council in Year 2000 Conversion, and charged agency heads with ensuring that the issue received the strictest attention. In October 1998, the Year 2000 Readiness and Disclosure Act was signed into legislation, requiring companies to share information with their constituents regarding preparedness and risk. Finally, the US Congress passed the Omnibus Consolidated and Emergency Supplemental Appropriations Act, 1999, which included \$3.35 billion in emergency funding for Year 2000 conversion activities.

Year 2000 requirements tripled the expense IT budgets were enduring in 1999, and testing consumed 50-70% of a project's time and resources. Most public and private institutions were finding themselves in the position—for the first time—of publicly sharing their business continuity and contingency initiatives. The millennium came and went without major technology glitches; and both regulators and technologists quickly turned their focus on other concerns. Now, however, we have seen a convergence of highly disruptive events that has galvanized the regulatory community again.

September 11, 2001

The coordinated attacks on New York and Washington, DC on September 11, 2001 was a straightforward assault on the American way of life—which included aggression toward the US government, military and economy. The transnational terrorists hoped to cripple us by damaging our economy, and they achieved some success.

"Our dependence on technology has grown such that technology disruption has become one of the requisite components when calculating operational risk."

The Fed Enables a Systemic "Soft Landing"

On September 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 raised the ceiling of a pre-existing swap with the Bank of Canada to \$10 billion.

Lloyd's of London estimated \$10 billion in corporate losses directly related to the business interruption the World Trade Center attacks caused. This is a staggering statistic in and of itself—but especially so when you consider the fact that Federal Reserve Vice Chairman Alan Ferguson prevented worse disruption when he authorized the injection of the US financial system with record amounts of liquidity a mere three hours after the first plane hit. Subsequent General Accounting Office (GAO) investigation into the financial markets' state of readiness revealed a certain laxity. Government officials worried not just about future terrorist attacks, but the ultimate effect on investor confidence.

Enron

While we were recovering from September 11, Enron Corporation, in a remarkably quick fall from grace, went from Wall Street favorite to the largest bankruptcy in US history. Furthermore, Enron executives were indicted for fraudulently manipulating earnings and stock prices, aided by outside advisers, including prominent accounting firms, investment banks and lawyers, in their crimes.

Even more stunning was the failure of the traditional system of checks and balances when it was disclosed that just four days before Enron reported a staggering \$618 million loss for the third quarter 2000—auditors from Arthur Andersen were directed to destroy all audit material, except for the most basic "work papers." As a result, investigators were denied access to thousands of e-mails and other electronic and paper files that could have helped illuminate the actions and motivations of Enron executives.

Corporate scandal: continuing pressure and escalating penalties

- *In response to cited email archiving violations of the Securities and Exchange Commission (SEC) Rule 17a-4 for record retention, five of the largest investment banks in the world agreed to pay a fine of more than \$8 million and achieve compliance in 90 days.*

Source: Wall Street Journal, August 2, 2002

- *The Securities and Exchange Commission settled enforcement action against Banc of America Securities LLC (BAS) for violations of recordkeeping and access requirements of United States securities laws. As part of the settlement, BAS agreed to a censure and a \$10 million civil penalty.*

Source: SEC press release, March 10, 2004

- *Symbol Technologies was fined a total of \$37 million for fraudulent accounting practices that had a cumulative net impact of over \$230 million on Symbol's reported revenue and over \$530 million on its pre-tax earnings.*

Source: SEC press release, June 3, 2004

- *Lucent Technologies paid \$25 million in penalties for fraudulently and improperly recognizing approximately \$1.148 billion of revenue and \$470 million in pre-tax income during its fiscal year 2000.*

Source: SEC press release, May 17, 2004

- *According to a study conducted by the American Management Association, The ePolicy Institute and security vendor Clearswift, 14% of organizations were ordered by a court or regulatory body to produce employee email in 2002—up 9% from two years prior. The research also found that only 34% of employers had an existing written email retention and deletion policy in place. This is the same figure reported in 2001, 12 months before five Wall Street brokerages were fined \$8.3m for failing to retain emails.*

Source: "Firms at risk on email legal liability," Robert Jaques, vnet.com, June, 18 2003.

Government response to concerns about cash flow and investor confidence

1929 Market Crash	Year 2000	9/11/2001	Enron 2001	2003 Blackout
First time financial regulations	First time regs requiring publication of continuity and contingency	First massive attack on US economy	Largest bankruptcy in US history	Largest blackout in US history
SEC established		Several risk, security availability regs established	Disclosure and compliance regs established	Contingency regs reinforced

Significant events and their impacts on regulatory compliance, 1929-2003.

The timing for this scandal could not have been worse for the US and NY stock markets, as it further shook investor confidence and tarnished the reputation of both Corporate America and public accounting. Successive scandals led to the inevitable focus on reporting integrity and executive accountability.

2003 Blackout

Further reinforcing the economy's dependence on technology was the 2003 Blackout. Just after 4 p.m. Eastern Daylight Time (EDT) on August 14, 2003, the North American power grid experienced a large-scale blackout that affected an estimated 50 million people and more than 70,000 megawatts (MW) of electrical load in parts of Ohio, Michigan, New York, Pennsylvania, New Jersey, Connecticut, Massachusetts, Vermont, Ontario and Québec. Although power was successfully restored to most customers within hours, some areas in the United States went without for two days and parts of Ontario experienced rotating blackouts for up to two weeks.

Safeguarding the financial services supply chain

To its credit, the financial sector, which serves as the backbone of the world economy, is on the forefront of best practices and innovative self-regulation. Rather than wait for recommendations and rules to be issued, many institutions are proactively developing and adopting best practices. In fact, individual organizations have been as groundbreaking in developing and implementing compliance and continuity solutions as the financial governing bodies have been prolific in drafting regulation. Not only is their need for compliance greatest when it comes to building investor confidence, but their risk of exposure is greatest. The financial sector is a fully interconnected economy, so protecting information and availability throughout its value chain is as critical as protecting the institution itself.

The cause of the blackout was determined to be a succession of miscues that included:

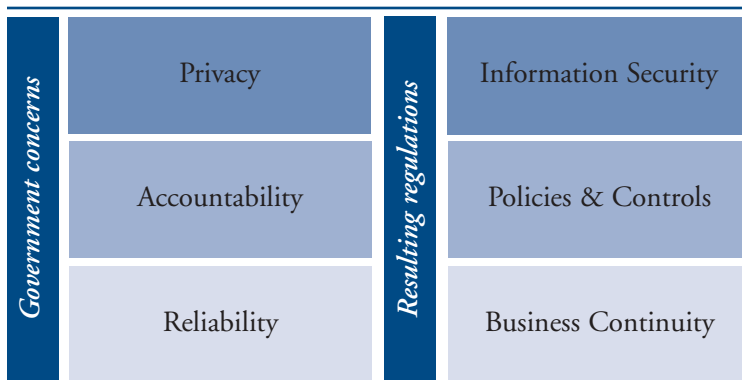
- FirstEnergy (FE) losing functionality of its critical monitoring tools, which resulted in a lack of situational awareness of degraded conditions on its transmission system
- FE not adequately managing tree growth in its transmission rights-of-way
- The Midwest Independent System Operator (MISO) reliability coordinator failing to provide adequate diagnostic support

- Coordination and communication between the MISO and Pennsylvania New Jersey Maryland Interconnection LLC (PJM) proving ineffective
- Several violations of the North American Electric Reliability Council (NERC) reliability standards

The largest blackout ever demonstrated that aging infrastructure can lead to widespread regional disruptions, which may become more common, according to government sources. Twenty First Century threats have escalated from statistically predictable natural calamities to new intentional or man-made disasters that occur irrespective of geographic locale.

Emergence of Convergence

Like the proverbial "perfect storm," this singular combination of events has changed the regulatory environment. SunGard has coined the phrase *Emergence of Convergence* to describe today's business and investor climate, where regulations and risk converge to elevated levels of continuity, security and data protection. Government concerns for reliability turn into business continuity regulations; privacy trepidation translates to information security regulations; and accountability concerns are addressed by procedural and controls rules as they relate to improved information lifecycle management (ICM).



Emergence of Convergence.

The Buck Stops Where?

Today's regulatory groundswell is the result of a general governmental unease with companies' risk management capabilities and the magnified impact that could result from deficiencies.

Regardless of the specific language or focus, each mandate is concerned with mitigating some component of exposure. For the first time in history, CEOs are being personally held accountable for the financial statements of their companies. CIOs can be indicted for not suitably reporting control breakdowns. And the Board of Directors is likely to encourage new levels of scrutiny resulting from their own increased individual accountabilities.

There will be continued evolution in responsibility and accountability. As the government prescribes and monitors a certain level of preparedness from industry, companies must react via policies and processes that achieve the required results.

New categories of risk force new levels of responsibility and accountability, which is, in essence, a convergence of organizational focus. Historically, a chief information officer (CIO) was focused solely on procurement and management of technology within the data center. Today's CIO, however, is faced with mitigating multiple risks that are rooted in globalization and extreme dependence on IT. Organizational exposure points include privacy and security concerns, the interconnected value chain and liability for service level agreement (SLA) failures. In other words, the CIO is tasked with devising and implementing tactical strategies for varied and far-reaching strategic organizational goals, including regulatory compliance.



Managing compliance is a cross-departmental effort.

Don't Divvy Up the Regs

The convergence of regulatory attention has left organizations faced with increased scrutiny by multiple agencies that have deployed multiple teams of auditors with parallel, but not identical, requirements. As with most "leaky pipe" situations, companies have solved individual regulatory challenges through an allocation of resources to deliver a specific result. This "one and done" approach to compliance contradicts the overall goal of ensuring ongoing efforts and monitoring improvements over time. To compound the problem, responsibility has been traditionally spread among siloed or departmental disciplines with different budgets, different staff and different levels of accountability. For some, there is no correspondence between their tactical, operational objectives and those of the business.

For example, the regulatory profile of a top-tier commercial bank might include the Interagency Paper on Sound Practices to Strengthen the Resilience of the US Financial System (Interagency Whitepaper), the Gramm-Leach-Bliley Financial Services Modernization Act (GLBA) of 1999, NASD Rules 3500, 3510, and 3520, the Securities and Exchange Commission (SEC) Rule 17a-4, the Sarbanes-Oxley Act (SOA) of 2002 and applicable retail regulations from the Federal Financial Institutions Examination Council FFIEC and the Office of the Comptroller of the Currency (OCC.) A healthcare organization, in addition to Joint Commission on Accreditation of Healthcare Organizations (JCAHO) oversight, will need to address GLB, the Health Insurance Portability and Accountability Act (HIPAA), and, if a publicly held company, SOA. There is content cross-over among regulations in multiple areas, especially on the topics of continuity and resumption strategies, and information security

and privacy. Not only are siloed efforts duplicated unnecessarily, but they also create the potential risk of inconsistent response.

Recurring Themes in Regulatory Compliance

More than one hundred papers, rules, and policies have been produced by dozens of domestic and international regulatory agencies in the last five years. Among the majority are these recurring themes:

1. Corporate executives are under unprecedented scrutiny
2. Operational risk has entered the regulatory lexicon
3. Privacy guidelines have become global

Executive Accountability

In an effort to ensure corporate responsibility and restore investor confidence, governing bodies are instituting rules that force corporate executives to take responsibility for internal controls and regulatory compliance.

Section 404 of SOA of 2002, for example, requires senior executives to personally attest to the accuracy of an organization's financial measurements and the controls that were implemented to ensure it. This requirement is landmark in the level of personal responsibility and accountability it places on a company's management team to ensure ethical and sound reporting in the public interest. And, it culminates in individual penalties for noncompliance that include fines of up to \$5 million and imprisonment of up to 20 years.

SOA's mandates echo the UK's Internal Control: Guidance for Directors on the Combined Code (The Turnbull Report) of 1999, which calls on boards of directors to regularly review reports on the effectiveness of the system of internal control in managing key risks, and to undertake an annual assessment for the purpose of making their statements on internal control in their annual report. Further, the Higgs Report of 2003 is a code specifically aimed at boardroom reform that may ultimately raise business continuity, emergency preparedness and disaster recovery to a higher level of corporate concern and attention.

For executives, a new level of attention means evaluating related systems and processes to determine what improvements are required in order to measure and report performance. To support their efforts, a new generation of support tools, such as compliance dashboards, will evolve to provide greater and immediate visibility into their compliance and risk status. In fact, compliance requirements should and will begin to affect overall technology strategy decisions and best practices in compliance will, in fact, deliver competitive advantage for those who attempt to leverage their benefits.

Operational Risk

Operational risk is a term used as early as 1988 in the Basel Committee on Banking Supervision (the first Basel Capital Accord)—and is often included with financial risks such as credit and liquidity. Operational risk, addresses strategic efforts to improve the consistency of internal process execution, reducing and preventing disruptions to business processes. The most significant causes of operational losses include

fraud, damage to physical and electronic assets, privacy and security breaches, and system failures.

The Basel Accords pertain to international banking and only affect the very largest US banks. Nonetheless, strong operational risk management serves as an excellent model for what other regulators are advocating. The SEC in particular has moved to tighten the reins on securities firms, issuing rules and guidance extended from primary clearing and settling to individual broker firms.

The regulatory publications listed below target business continuity, information security and the integrity of record retention as critical elements of their requirements. Their intent is to improve resilience, transparency and accountability in order to minimize operational risk for the entire trading cycle, with the resulting benefit of improving investor confidence.

- Interagency White Paper. SEC, OCC and Federal Reserve, April 2003. Compliance: 2004. Target audience: Wholesale clearing and settling firms.
- SEC Policy—Business Continuity for Trading Markets, draft 2003. Compliance: 2004. Target audience: Self regulated market exchanges, electronic communications networks (ECNs) and market data feeds.
- NASD Rule 3510. Compliance: 2004. Target audience: Registered broker members of the National Association of Securities Dealers (NASD); introduced customer disclosure for recovery strategies and senior manager accountability. Similar to New York Stock Exchange (NYSE) Rule 446.

- SEC Rule 206(4)-7 and Rule 38a, approved February 2004. Target audience: registered investment advisors (RIAs) and investment companies; requires the addition of a Chief Compliance Officer.
- SEC Proposed Rule 203(b)(3)-2, drafted July 2004. Target audience: Hedge fund advisers; must now register with SEC and implement a compliance program like those of RIAs.

As the economy continues through its recovery, business initiatives, such as straight-through transaction processing, will increase. And as new technologies are adopted and deployed in business-critical environments, the regulatory community will undoubtedly address their impacts on continuity. Industries, such as manufacturing and healthcare, that are heavily dependent upon technology and have regulatory exposure should look to the financial services industry's experience as "a canary in the mineshaft" and plan their operational risk strategies accordingly.

Privacy

Privacy guidelines aimed at protecting the confidentiality, integrity and accessibility (CIA) of the personal data of private citizens and consumers are becoming ubiquitous. While the Internet promises to revolutionize the way governments and businesses serve their "customers," the potential for abuse and fraud is high. As such, consumers are literally clamoring for assurances that their personal data is protected and secure—and governments are responding with a plethora of privacy laws.

It is in the privacy area that the cumulative nature of regulations is most obvious. Most build on others, helping parties comply with an existing rule and/or plugging apparent holes in another. The list is growing quickly, but the following are the most important privacy guidelines to date:

- The European Union Data Protection Directive, Directive 95/46/EC, 1995—Covers processing of personal data wholly or partly by automatic means and processing otherwise than by automatic means, which form part of a filing system or are intended to form part of a filing system.
- Health Insurance Portability & Accountability Act (HIPAA), 1996—Outlines necessary "administrative, physical and technical safeguards to protect the confidentiality, integrity and availability of electronic protected health information," requiring covered entities (CEs) to implement basic safeguards to guard "electronic protected health information from unauthorized access, alteration, deletion and transmission."
- Section 501 of the Gramm-Leach-Bliley Financial Services Modernization Act (GLB or GLBA), 1999—Requires financial institutions (defined as banks, thrifts and credit unions, as well as numerous non-depository institutions) to develop a written security plan that describes their protection programs for customer information (defined as any record containing nonpublic, personal information about a customer, whether in paper, electronic or other form, that is maintained by or on their behalf.)

- US Department of Commerce's Safe Harbor Framework, 2000—Provides a streamlined means for US organizations to comply with the European Union's Data Protection Directive.
- Personal Information Protection and Electronic Documents Act (PIPEDA), Canada 2000—Applies to traditional, paper-based business, as well as on-line commercial activities with regard to information about an "identifiable individual that includes any factual or subjective information, recorded or not, in any form."
- Various state consumer information protection "like" rules, including California Civil Code 1798.80, AB 2246 and California SB 1386—Provide the best evidence to date that private citizens are making inroads with their legislators and policymakers regarding security and protection concerns.

There are also evolving trends concerning cross-border data transfer due to differing jurisdictions for privacy laws. Organizations would be wise to regularly monitor security and privacy guidelines to update policies and compliance procedures.

Responsibilities in Economic Preparedness

The regulatory climate has presented new challenges for all of us. While the ultimate goal is to build a safer, more stable global economic infrastructure, the path to get there poses challenges for executives in every organization. Many struggle with understanding just exactly what metrics will be used to determine a successful effort. The sentencing guidelines for US District Courts and legal counsel have identified the following as key accountabilities and performance metrics:

- "Tone at the top" and leadership accountability
- Established policies and procedures
- Properly communicated standards
- Effective measurement
- Consistent enforcement
- Response and prevention

The governing bodies have made it clear—compliance is directed at the management layer to ensure penetration throughout the entire organization. And, it is most effectively carried out via a top-down, enterprise-wide effort that leverages a multi-discipline pool of talent to identify exposures and builds best practices.

Can there possibly be a payoff?

Let's be honest, spending money to satisfy the requirements of regulatory compliance can be tough enough to swallow, but attempting to show a return on investment (ROI)? Impossible? The truth is many companies are, in fact, recognizing some levels of return on their compliance investments made in the past 12 months. One senior executive noted that a more resilient infrastructure delivered a clear competitive advantage, while another was able to deploy programs less expensively using a holistic approach (versus scattered, one-off efforts.)

Conclusion

SunGard has coined the phrase Emergence of Convergence to describe today's business and investor climate, where regulations converge to elevated levels of continuity, security, and data protection and new categories of risk have forced new levels of responsibility and accountability. The myriad of regulatory demands affecting companies is best served by an overarching program that takes a holistic approach to corporate governance.

Finding an Experienced Partner

Integrating business continuity, information security and information management is no small task. Often, organizations benefit from expert, third-party assistance. When seeking a partner, consider firms that offer extensive experience in the three separate areas. It is also helpful to engage a partner that has demonstrated skill in identifying, adopting and deriving best practices from industry rules and regulations.

Working with a partner, such as SunGard, provides:

- An comprehensive enterprise perspective
- The peace of mind that comes from working with a trusted partner
- Third-party objectivity in developing best practices that address multiple regulatory concerns
- Access to extensive and proprietary industry benchmarking information
- A holistic methodology that leverages all relevant disciplines and includes information security and disaster recovery
- A demonstrated clean chain of custody

SunGard can help develop an overarching and enterprise-wide approach to risk mitigation and incident planning as they relate to corporate governance. SunGard offers a complete array of services to help organizations assess risks, integrate their business continuity, information security, and information management plans, continually test and improve their consolidated plans, and implement them with an eye toward regulatory compliance.

SunGard's team of experts help eliminate identified concerns through targeted risk mitigation services, which address such issues as policies and procedures, architecture, internal controls, monitoring and measuring and awareness. In short, we help clients elevate their thinking and plans by incorporating critical corporate governance issues into their comprehensive information availability plans.

To get started today on assessing your corporate governance program, visit our website at www.availability.sungard.com or call our information availability experts at 1-800-434-0002.

About SunGard Availability Services

From initial assessments and plan development through execution and ongoing management, **SunGard Availability Services** offers a one-stop source for helping organizations integrate risk management and incident response into their information availability plans.

SunGard Availability Services delivers solutions to support information availability—keeping people and information connected no matter what. Information availability requires not only technology, but also people, processes and physical infrastructure. Therefore, SunGard offers a full continuum of **managed IT**, **professional** and **business continuity** services:

- SunGard's **managed IT services** provide a secure, reliable environment to host mission-critical systems and applications. Offering a full portfolio of outsourcing, hosting and support services, SunGard gives clients the option of point or turnkey solutions.
- From assessing needs to designing solutions, our **professional services** help clients address availability challenges. We deliver information security, high availability and business continuity services, as well as services designed to help clients address regulatory requirements. We also deliver SunGard Paragon™, a next-generation Information Availability planning software tool.
- With one of the most extensive infrastructures in the industry, SunGard also delivers **business continuity services**. From traditional hotsites to leading-edge high availability solutions, our offerings enable clients to cost effectively meet all availability requirements.

SunGard Availability Services is an operating group of SunGard (NYSE:SDS), member of the S&P 500. With more than 25 years of experience helping organizations ensure information availability, we are uniquely positioned to provide vendor-independent recommendations and solutions. For more details on our services, visit our website at www.availability.sungard.com or call 1-800-434-0002.

Authors

Contributing and Managing Editor:

Pat McAnally, Senior Director, Thought Leadership Program

A veteran of the business continuity industry for more than a decade, Pat McAnally is a published author, speaker and subject matter expert on information technology and the impact of new regulations. McAnally's work has been cited in case study material by Bitpipe (syndicator for 90 top technology analyst firms) for the successful use of intellectual capital in generating awareness. She currently heads SunGard's Thought Leadership program, focused on bringing the intellectual capital and experience of SunGard's team of 2,000 global experts to the IT community.

SunGard Availability Services

SUNGARD[®]
Availability Services

680 East Swedesford Road
Wayne, PA 19087
484.582.2000
800.434.0002
www.availability.sungard.com

© 2004 SunGard Availability Services. All rights reserved.

The above material is presented as general information only and does not constitute legal advice or a legal opinion. You should seek the advice of legal counsel with respect to your particular circumstances.

OS-004