

An Information Availability Primer

for Executives of
Small and Midsize
Businesses



Introduction

From creating operational efficiencies to enabling new business models, technology is now a driving force across industries. And, that's true for more than just the corporate giants. Small and midsize businesses have also embraced the power of technology—and, more importantly, the value of the information it stores, transmits and processes.

Indeed, information—not data alone—is the lifeblood of every business. Your organization's ability to survive and thrive is contingent upon your ability to deliver optimal information access.

Quite simply, you need to know that no matter what happens inside or outside your “four walls,” your business will *stay* in business.

Understanding Information Availability

Information Availability solutions deliver the secure data, systems, networks and support you need to keep your business in business. Effective solutions result from careful planning, design, implementation and management of your entire IT infrastructure.

Information Availability requires a resilient architecture that keeps people and information connected—all the time, no matter what. That architecture should be based on proven industry standards and best practices. And it should deliver always-on, always-ready power, networks and systems. Of course, any IT infrastructure includes not only technology assets, but also the people who use it and the processes it supports.

With that in mind, you simply can't think of Information Availability as a one-time project. Rather, consider it an ongoing program—and a framework to guide virtually every decision you make about your information and the supporting technology infrastructure.

In case you're feeling overwhelmed about the complexity and expense of an Information Availability program, consider the benefit of third-party support and solutions from an expert provider, such as SunGard Availability Services. SunGard's mission is keeping people and information connected. We've helped thousands of organizations develop strategies and design solutions that provide the information access their businesses require.

In this primer—developed especially for small and midsize businesses—SunGard walks you through the nine major areas that comprise an Information Availability program.

The “building blocks” of Information Availability

If you were to assess your current approach to Information Availability—however formal or informal—you might identify strengths in certain areas. Perhaps you’ve analyzed and addressed system interdependencies or

have a strategy for information lifecycle management. But, chances are, there are some areas where you need to improve—and some that you haven’t addressed at all.

Consider how your organization is—or isn’t—addressing your needs in each of the following areas:

- 1. Disaster recovery*
- 2. Continuity and testing*
- 3. E-mail*
- 4. Data and records management*
- 5. Network*
- 6. Facility and environment*
- 7. Security*
- 8. Policies, procedures and regulatory compliance*
- 9. Training and awareness*

1.

1. Disaster recovery

Perhaps the most basic component of an Information Availability program is a sound approach to disaster recovery (DR). And yet, many organizations still do not have proven strategies and tactics for backing up—and recovering—their systems and data.

In case September 11, 2001, didn't get your attention, Hurricane Katrina should have. Both of those events—one manmade, one a natural disaster—further underscored the absolute necessity of DR. So, if you already have provisions for DR, re-evaluate and test them. Make sure your current plan would, in fact, support the recovery of your IT systems. And if you don't have a formal DR plan, it's time to develop one. You simply can't afford not to.

Key considerations:

- In what ways is your organization dependent upon your IT infrastructure?
- Have you identified interdependencies and calculated the potential financial impact of losing access to your critical systems and data?
- What is your current approach to DR? When was the last time you updated your written plan and/or tested it?
- What are your current provisions for an alternate data center? If you have a hot site contract, when was the last time you assessed it to ensure that it would support a full recovery of your critical IT systems?

How SunGard Can Help

SunGard offers a full complement of traditional disaster recovery services—including hot sites, cold sites, mobile recovery and end-user recovery solutions. In addition, our Professional Services team has deep experience and expertise in performing Business Impact Analyses (BIAs), as well as in writing, maintaining and testing formal DR plans.

S I D E B A R

RTO and RPO

Before you can develop an effective plan, you must first identify your business's recovery time objectives (RTO) and recovery point objectives (RPO).

An RTO dictates how quickly you need to recover your business. It's the amount of time that elapses from the point at which a disruption occurs until the specified business operation is restored and current business transactions can be applied. Your RTO may vary among your business processes and/or applications. In other words, you may assign an RTO of less than one hour to your most critical applications while targeting recovery within 24 hours for less critical systems.

An RPO measures the amount of potential data loss in number of hours from the time of interruption. You need to identify how much data you can "afford" to lose. For example, your key, mission-critical systems may have an RPO of 15 minutes—meaning that you would lose only 15 minutes' worth of data.

Only by clearly identifying your RTO and RPO for each of your processes and systems can you select and implement continuity solutions that effectively balance cost and risk.

2.

2. Continuity and testing

Every business needs a clear, actionable plan for ensuring continuity of services. But simply writing such a plan isn't enough. Ideally, your organization should approach continuity as an ongoing effort. Only then will your plan reflect ever-evolving business conditions—including internal, as well as external, changes.

As part of maintaining your continuity plan, you must test it—rigorously—on a regular basis. At SunGard, we advise clients not to plan their test, but to test their plan. In other words, strive to execute tests that are highly realistic. Create scenarios that reflect the challenges and complexities of the “real world.” That way, you'll be truly prepared to stay in business following any interruption—from natural disasters to power outages to labor strikes.

Key considerations:

- Does your organization have a formal program for continuity planning and testing?
- Do you have a documented, actionable plan? When was the last time it was updated?
- What kind of challenges do you face when it comes to keeping your continuity and availability program on course?
- What is your formal approach to continuity testing? Do you plan your tests—or test your plan?
- Does the test program include documented policies and procedures? Does it define employee roles and responsibilities? Is all of this communicated to employees?
- How does your plan address interdependencies with members of your value chain?
- Has your continuity program ever been validated by an objective third party?

How SunGard Can Help

Every year, our continuity and availability experts spend some 350,000 hours helping companies like yours to create and improve their continuity programs. In fact, SunGard has helped write more than 10,000 continuity plans. We help clients perform over 9,000 testing exercises annually. And SunGard Paragon™, our software package, is an industry-leading tool for planning and maintaining Information Availability.

3.

3. E-mail

Although e-mail applications traditionally haven't been regarded as "strategic" in nature, they've become mission-critical for today's small and midsize businesses. When e-mail service is disrupted, a vital channel for internal and external communication goes down. And, Information Availability—along with your business—grinds to a halt.

Adding to the challenges are external actors—such as viruses, spam and phishing—that continually threaten e-mail security and availability. And, of course, regulations now require that certain messages be archived in compliance with various mandates, such as the Sarbanes-Oxley Act.

And yet, you may be struggling with the best approach to ensuring the availability, continuity and security of your e-mail system.

Key considerations:

- How do you currently manage e-mail? How much of your IT staff's time is spent on day-to-day maintenance tasks?
- Have you assessed the impact of e-mail downtime? Do you have an RTO and RPO for this application?
- What are your current provisions for ensuring the continuity and availability of e-mail?
- What regulatory and/or discovery requirements do you face? How do you currently back up e-mail data? Are you archiving?

How SunGard Can Help

SunGard offers an end-to-end suite of cost-effective solutions that can help you protect, maintain, archive and recover your e-mail system. We also deliver an Archiving Service for Messaging to help companies—especially in the financial services industry—to address specific compliance requirements.

4.

4. Data and records management

Many companies wrestle with how to identify and differentiate types of data. What is critical data versus non-critical data and how do you recognize it? More importantly, what does each classification mean to you—now and in the future?

All stored information has value. However, what was highly used, valuable and critical at one time can quickly fall out of importance. Thus, information may be disposed of once it serves no governmental, legal, institutional or evidentiary purpose.

With the right combination of formal analysis and documented guidelines for classifying data, you have the necessary ingredients for a comprehensive data retention, disposal and recovery plan. Such formal policies and procedures become institutional law and help avoid the eventual drift that occurs with the absence of clear-cut criteria and directed action. Meanwhile, off-site rotation provides an additional layer of protection.

Key considerations:

- Do you have a well-developed, formal policy statement regarding vital records? Has it been reviewed and approved by management?
- Is there a training and awareness program regarding the importance and procedures of the policy statement?
- Has a formal analysis of critical versus non-critical data been conducted? Are the off-site schedules for critical data formally defined?
- Has IT performed a formal analysis to determine the most effective and efficient method for backup and recovery? (See sidebar for more information.)
- Has recovered data been verified as complete?

How SunGard Can Help

With a focus on information lifecycle management, SunGard offers professional and managed services to help you tackle the complexities of data and records management. We also deliver advanced solutions to improve the speed, reliability and efficiency of your backup process.

S I D E B A R

The Basics of Backup

There are two primary methods of backup: traditional tape backup and vaulting via a remote connection.

As the name suggests, tape backup involves saving a copy of your data to a physical medium. Every tape should be sent to and stored in a safe, secure, off-site location.

The trouble with tapes is that they can get lost in transit and it's often difficult to verify that backups have occurred as planned. What's more, the tapes themselves can fail—or be discontinued, making long-term access to backup data a challenge.

Vaulting is a newer, faster and more efficient alternative to traditional tape backup. It enables you to simultaneously back up your data and move it offsite, where it can be stored safely and securely.

SunGard's Vaulting for Distributed Systems is a cost-effective managed service that can help you take control of your backup processes. SunGard delivers automated status reports that your IT managers can access anytime, anywhere using a standard web browser.

5. Network

Your network is the link that keeps your business connected. It's critical to your customer and partner communications, business transactions and processes, and overall operational efficiency. In fact, a 24x7 network connection is essential to organizational productivity and longevity. Therefore, your Information Availability program should help your organization ensure a continuous data communication link while addressing:

- Redundancy, including network failover capabilities
- Diversity, providing fundamental dissimilarity between redundant networking features and technology
- Recoverability, including assurances that communication is capable of being resumed

Key considerations:

- How critical is it that your employees have access to main systems and applications?
- What are the main systems and applications in order of priority?
- How dependent are they upon network communications?
- How much will it cost your business to *not* have guaranteed connectivity?
- Will your chosen networking technology have redundancy configured in? If not, how can you achieve it?
- Who are the members of your supply chain and what are their connectivity requirements? What are their contingency plans?

How SunGard Can Help

Underpinning all of our Managed IT and Business Continuity services, the SunGard Global Network (SGN) was designed to provide the ultimate in redundant connectivity. SGN makes industry-leading network availability accessible—and cost-effective—to companies regardless of their size.

6.

6. Facility and environment

Physical assets—your office space, data center and other facilities—are critical to keeping your business on track. And, companies sometimes make dangerous assumptions about their ability to get back into their facilities. Then, when a disaster or other interruption occurs, they realize—too late—that they don't have a workable alternate site to meet their true Information Availability needs.

Does your organization have a viable backup site? If you're depending on an "internal" backup facility, make sure that it offers enough capacity and that it mirrors your primary site. In addition, your data centers—both the primary and secondary locations—should be hardened. That means redundancy across all major areas, from cooling systems and fire protection to physical security.

Key considerations:

- Have you re-evaluated your facilities and equipment management strategy within a post-9/11 world?
- Do you have organizational buy-in regarding your definition of facilities and equipment management and associated responsibilities?
- What are your minimum personnel and equipment requirements—and what is the theory behind those determinations? Have you documented your requirements?
- Have you included them in your overall recovery plan and performed testing on them?
- Do you have formal procedures for conducting damage assessments? Are they standardized and documented in recovery plans?
- What sort of site selection criteria did you use for each of your locations? Did you consider hazards, such as flood plains and air traffic patterns?
- What sort of building access control and security do you employ?

How SunGard Can Help

SunGard has made significant investments in redundant, hardened facilities—so you don't have to. Our End-user Recovery Services provide cost-effective—and highly reliable—alternate facilities to get your people back in business following a disaster or other interruption. In addition, we offer Mobile Recovery Services that bring an alternate workspace to you.

7. Security

As a small to midsize business, you may find your resources too limited to deploy extensive human resources and invest heavily in security products and services. And even if you could, that wouldn't necessarily eliminate the information security threats you face—including unauthorized access to a system or data; disruption or denial of service (DOS) attacks; unauthorized use of a system for the processing or storage of data; or unauthorized changes to system hardware, firmware or software characteristics.

Your Information Availability challenge is two-fold: to ensure the confidentiality, integrity and availability of mission-critical systems and data resources and to safeguard your people and facilities against physical threats. That's why the most effective approach for staying on top of physical and cyber threats is an integrated, enterprise-wide security program. Only then can you implement the right policies, processes and procedures to address existing and emerging threats.

Key considerations:

- What's the minimum security you need to protect your business?
- Do you conduct annual IT security risk assessments?
- Have you established a consistent process to request, authorize and grant access to systems, databases and applications?
- Do you have routine indicators to monitor your overall IT security infrastructure?
- Do you perform daily or weekly reviews of pertinent security audit logs?
- Have you established information security access models?
- Have you instituted building and data center physical security practices? Is the building staffed 24x7 by an independent security organization?
- Are security alarms and cameras monitored by that staff? Are all building doors alarmed and solely accessible through an access system (card, biometric or other)?
- Is an electronic log of all access maintained and periodically reviewed by management?

How SunGard Can Help

Offering third-party objectivity, SunGard's team of experts can help you develop, implement and maintain a programmatic approach to information security. You may also want to consider our suite of Managed Security Services for continual identification and proactive resolution of security issues.

8.

8. Policies, procedures and regulatory compliance

Government agencies and international bodies have a vested interest in maintaining financial stability and investor confidence. That's why they're taking no chances when it comes to ensuring appropriate Information Availability measures and levels within private industry. Concerns for reliability turn into business continuity regulations. Privacy fears translate into information security regulations. And accountability issues are addressed by procedural and controls rules as they relate to improved information lifecycle management.

Businesses of all sizes are faced with significant challenges in the area of regulations for privacy, security, continuity and records management. New categories of risk are forcing new levels of responsibility and accountability—and that means you need to have a cross-functional approach to policies, procedures and regulatory compliance.

Key considerations:

- How does your organization currently approach policies, procedures and regulatory compliance?
- In general, are you reactive (focusing on meeting immediate deadlines and requirements) or proactive (building a company-wide program that can meet a variety of needs)?
- Do you perform regular compliance audits of IT controls?
- Does a testing schedule exist? Is it shared across the organization? Does it include all areas of the business continuity program—including people and processes?

How SunGard Can Help

SunGard offers a variety of services to help support the development and ongoing maintenance of policies and procedures. In addition, our Regulatory Compliance Review can help to assess your current state and identify actionable areas for improvement.



9. *Training and awareness*

Training and awareness is one of the most important—and also most overlooked—building blocks of an Information Availability program. After all, plans are only effective if they are used properly. Effective execution requires communication and understanding—the hallmarks of education.

As with any internal initiative, an Information Availability plan requires visible and vocal management support, as well as clear, consistent information exchange. As a small or mid-size business, you may be able to conduct highly personalized training. Or, if your employees are geographically dispersed, it may be more cost-effective to use Internet conferencing or other web-based communications vehicles. Whatever methods you use, be sure that your communications are clear, consistent—and ongoing.

Key considerations:

- How do you currently inform employees about your organization's Information Availability strategy?
- Are all of your employees well-versed in your information security, data records and storage, and business continuity policies?
- How do you ensure that new employees are educated and informed about your organization's policy?
- How do you involve all employees in testing and other activities related to continuous improvement of your Information Availability program?
- How will your employees communicate with each other in the event of a disaster?

How SunGard Can Help

SunGard offers Incident Response Training and Security Awareness Training services—both of which can help you better prepare employees for disasters, security breaches and other interruptions to your business.

Conclusion

For technology-dependent enterprises of all sizes, it's never been more important to ensure that your Information Availability solutions deliver the secure data, systems, networks and support your business requires.

When your employees, customers, suppliers or partners can't gain access to the information they need, your business suffers. But, protecting that access isn't as simple as installing redundant hardware or creating a business continuity plan. In fact, ensuring true Information Availability requires a holistic view of your business and the infrastructures that support it. It also requires you to have a firm handle on the nine components discussed in this primer.

Assessing your existing infrastructure is the first step in improving it. A comprehensive review, along with comparative and gap analyses, are essential components of such an evaluation.

Many organizations find tremendous advantage in enlisting the help of an experienced third party. At SunGard Availability Services, we've helped thousands of clients to build, improve and maintain Information Availability programs. And we don't just work with "corporate giants." In fact, we have a suite of services and solutions designed for small to midsize businesses like yours.

Get Started Today

To learn more about how SunGard Availability Services can help you assess and improve your Information Availability program, call 800-468-7483 or visit us online at www.availability.sungard.com.

About SunGard Availability Services

SunGard Availability Services is the pioneer and leading provider of Information Availability solutions that deliver the secure data, systems, networks and support clients need to stay in business. We enable more than 10,000 clients worldwide to keep people and information connected through customized enterprise-wide solutions that support people, processes and infrastructure. We provide a complete portfolio of Information Availability solutions using over 3 million square feet of secure, redundant facilities supported by a 25,000 mile global network, 25 years of experience and over 2,000 expert resources in managed IT, professional and business continuity services. SunGard is known for helping customers get back in business quickly after an unplanned event. We're also the best qualified to help ensure that businesses never go down in the first place.

Contributors

The following SunGard experts contributed their insight and experiences to this primer:

Frank Casey

Bill DiMartini

Carl Herberger

John Loughlin

Lenny Monsour

Pat McAnally

Chuck Resnick

SUNGARD®
Availability Services

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

© 2005 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.

SG-PRM-001