## Continuity, Consolidation and Compliance

# *Business Drivers for High Availability*

## White Paper

***Vision Solutions, Inc.***

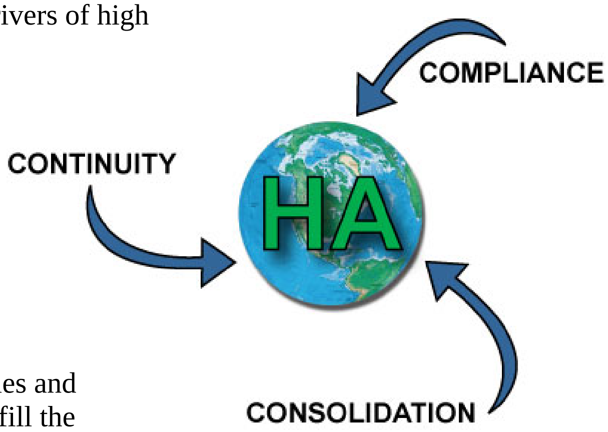
## Introduction

How long can a modern organization *operate* without critical information and applications? How long can a modern organization *survive* without critical information and applications? While the answer varies with every organization, as the dependency on information technology continues to grow, organizations' tolerance for interruptions to their information technology usage shrinks at least proportionately.

We live in an information age. Whereas, in the past, economic success depended upon access to raw materials and labor, today few organizations can operate at anywhere near full capacity, if at all, without their data and applications. Most cannot survive long disruptions. Yet, as recent natural disasters have highlighted, the threat of downtime seems unavoidable—it isn't.

The concepts of survival and predictable operations have driven 'high availability' technology; technology that limits planned and unplanned downtime and enables disaster recovery, thereby reducing the inherent threat to data and information availability.

In this paper, we examine the following three drivers of high availability:



1. **Business Continuity**: The plans, processes and technologies that enable organizations to survive if parts of the organization are unavailable, damaged or destroyed.

2. **Business Compliance**: The activities and technologies adopted in order to fulfill the legal requirements of legislation, industry guidelines and the organization's service agreements regarding the safeguarding of operations and services.

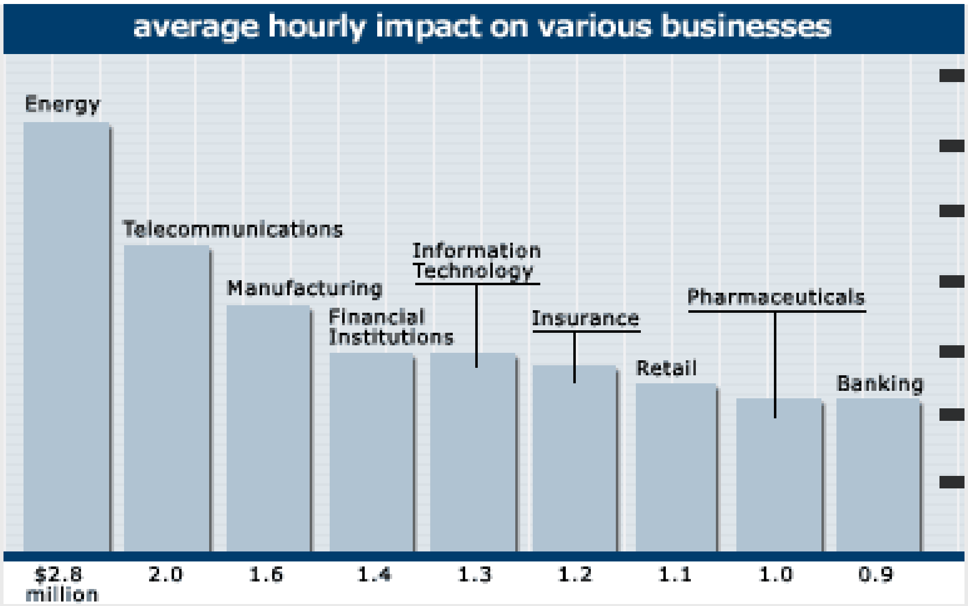
3. **Business Consolidation**: The economic and operational pressures encouraging organizations to simplify processes and systems which, in turn, introduces issues affecting business continuity.

These drivers, which present numerous challenges to organizations, compel a central tenet; *organizations cannot operate or fulfill their duties to customers or investors without predictable access to their critical business applications and information*. Most organizations are not prepared for moderate to catastrophic disasters and have limited provisions in place to ensure information and application continuity. A moderate natural disaster could severely interrupt operations and jeopardize an organizations' financial health and potentially its ability to survive. This white paper examines these issues and suggests a solution.

## Continuity

Recent extreme weather and tectonic events, coupled with terrorist activity, and the apparent increasing frequency of both, have sharply focused business leaders' thinking on the need for strategies and tactics to preserve the continuity of business operations should disaster strike. Should the worst happen, a business caught unprepared and without contingency plans in place and ready to be executed may not survive.

The threat to the business is more than just hyperbole. A classic study performed at the University of Texas at Arlington, *Financial and Functional Impact of Computer Outages on Business*, found that 90% of all businesses go bankrupt within two years after a significant computer failure. Unless adequate backup facilities are in place, the effects of a catastrophic event would certainly fall within the study's definition of a "significant failure." As shown below, the hourly cost of downtime is very significant:



Source: *IT Performance Engineering & Measurement Strategies: Quantifying Performance Loss, Meta Group, October 2000.*

Most organizations underestimate the true cost of downtime. As the above chart shows, when you consider all costs—immediate lost sales, long-term revenue loss due to degradation of customer loyalty, overtime costs needed to recover from the outage, penalties due to missed reporting deadlines and unfulfilled shipping guarantees, and more—the total cost to the business from as little as one hour of downtime can be staggering.

Catastrophes capture the headlines and their potential business impact is enormous, but they are rare. More frequent are less harsh events that, nonetheless, can have a significant impact the business. With today's near complete dependence on information technology and the electronic storage of data, even just one failed disk drive or server, or simple human error, can imperil a business' operations unless protective measures are in place.

Given enough time, every business will suffer some a potentially crippling system or data interruption. Because these events are rare or, in the case of catastrophes, exceptionally rare, some organizations may be prepared to accept the risks. Nonetheless, one type of event that typically forces systems and data offline is both frequent and mandatory: system maintenance. On a regular basis systems need to be shut down and data taken offline in order to backup and reorganize databases and upgrade hardware and software.

There was a time when maintenance could be scheduled during off-hours. However today, as databases grow, many of these activities have expanded to exceed the time available in traditional off-hour windows. Worse, these windows are shrinking.

With the advent of e-commerce, globalization and intensified competition, many more companies now operate around the clock than ever before. For them, there are no off-hours. Now any downtime, at any time, whether planned or unplanned, is unacceptable.

- ✓ At what point is the survival of your company at risk? 40% said 72 hours, 21% said 48 hours, 15% said 24 hours, 8% said 8 hours, 9% said 4 hours, 3% said 1 hour, 4% said within the hour. *(Source: 2001 Cost of Downtime Survey Results, 2001.)*

Increased global competition is another driver behind an increased focus on business continuity. As competition intensifies, not just from the local competitors, but, thanks to globalization, from around the world, companies must concentrate on lowering costs while improving customer responsiveness. Information technology is an important factor in achieving both. Keeping systems, and therefore the business, running is, consequently, a critical success factor in this more competitive environment.

Another trend driving the need for enhanced business continuity is the move toward garnering greater efficiencies in the supply chain. To achieve these efficiencies, the systems of entire supply chains are becoming integrated through the use of protocols such as EDI and Web Services. Many companies now depend on the seamless, paperless flow of information—design documents, inventory availability data, orders, shipping documents, order status information, invoices, payments, and more—between themselves and their customers and suppliers to keep their businesses flowing. An unavailable system no longer imperils only the company that owns it. System unavailability may threaten the operations of other companies up and down the supply chain.

## Compliance

Thanks in part to the accounting scandals of a few years ago and intensified concerns regarding security, businesses face a more stringent regulatory environment than in the past. Some of the new laws affect all businesses, some just public companies, while others are restricted to particular industries, but they all place an added strain on the affected businesses. A number of these regulations, including Sarbanes-Oxley (SOX), the Basel II accord, the Basel Committee's Capital Adequacy Directive (CAD III), the Gramm-Leach-Bliley Financial Services Modernization Act, and the Health Insurance Portability and Accountability Act (HIPAA), among others, require that organizations pay closer attention to protecting the integrity and availability of their business data.

The upshot of this legislation is that organizations must proactively take steps to ensure that data is protected and available.  High availability provides the means for organizations to help prevent information destruction from natural or man-made events.

Failure to comply is not an option. The financial penalties for non-compliance can have a very material affect on a company's profitability and, depending on the law that is broken and nature of the infraction, the penalty could also include jail sentences for the company's senior executives.

Below is an overview of the legislation that is relevant to high availability. This is not intended as legal advice. If you are involved in your organization's compliance programs, you should consult an attorney for more information on your legal obligations.

## *Sarbanes-Oxley*

The Sarbanes-Oxley Act was enacted to fight corporate fraud. Massive financial deception at Enron®, WorldCom® and Global Crossing® led to the passing of this legislation in 2002. The SEC is responsible for enforcement of Sarbanes-Oxley. Its rules dictate that all publicly traded companies must report yearly on the effectiveness of their financial controls. Accordingly, corporate governance has become a critical operational focus of organizations to ensure that they have the proper controls and audit processes in place to prevent and detect fraud.

The legislation has significant consequences for non-compliance. This includes civil and criminal penalties. Section 302 specifies that CEOs and CFOs are responsible for the accuracy of their company's financial reports.

The key portions of Sarbanes Oxley regarding high availability are Sections 404 and 409. Section 404 requires management to specify their responsibility for financial controls and report on the adequacy and shortcoming of the controls. Section 409 requires the timely reporting of financial information.

The role of high availability is to ensure the best availability of the most complete and accurate information for financial reporting, audits and fraud investigations. High availability allows organizations to exhibit best practices relevant to effective controls and provides immediate access to information for timely reporting.

**Links:**

- **U.S. Securities & Exchange Commission Spotlight on Sarbanes-Oxley Rulemaking and Reports:** http://www.sec.gov/spotlight/sarbanes-oxley.htm

- **Full act:** http://www.sec.gov/about/laws/soa2002.pdf

## *Basel II Accord*

The Basel II Accord is a set of international banking sector regulations that applies to all European banks and investment firms. In the United States it will, at least initially, apply only to the most internationally important banks, a group that numbers about 20.

The Basel II regulations, which will be applied in stages in 2006 and fully enforced in January, 2007, is designed to adjust banks' regulated capital requirements to better accommodate the perceived risks that the banks run, thereby reducing the risk to their viability. As a part of achieving this objective, Basel II specifically requires that banks protect the availability of their data. Furthermore, the Basel Committee's Capital Adequacy Directive (CAD III) requires that banks have information about their assets and associated risks readily available. As stated in a July 2003 background document produced by the Basel Committee, "Banks should have effective capacity, business continuity and contingency planning processes to help ensure the availability of e-banking systems and services."

**Links:**

- **U.S. Federal Reserve Board links page:** http://www.federalreserve.gov/generalinfo/basel2/default.htm

- **Basel Committee on Banking Supervision:** http://www.bis.org/bcbs/index.htm

### *Gramm-Leach-Bliley*

Gramm-Leach-Bliley or The Financial Modernization Act of 1999 or simply GLB, has a broad spectrum of qualifications, requirements and regulating parties. Eight agencies and the states are charged with managing and enforcing the regulations.

GLB applies to financial organizations or any organization that collects or transfers private financial information for the purpose of doing business or providing a service to its customers.

The two regulations of GLB are the Financial Privacy Rule and the Safeguards Rule. The Financial Privacy Rule addresses the collection and dissemination of customers' information while the Safeguards Rule governs the processes and controls in an organization to protect customers' financial data.

The Safeguards Rule is enforced by the Federal Trade Commission. In addition to the public embarrassment of non-compliance, organizations may be fined thousands of dollars a day while they are non-compliant.

The Safeguard Rule of GLB calls for financial institutions to:

1. Ensure the security and confidentiality of customer information

2. Protect against any anticipated threats or hazards to the security or integrity of such information

3. Protect against unauthorized access to or use of such information that could result insubstantial harm or inconvenience to any customer

To ensure that customer data is protected against threats and to ensure its integrity, financial institutions must protect against the destruction of customer and account data whether from equipment failure, disasters or human error.

**Links:**

**Full act:** http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=106_cong_public_laws&docid=f:publ102.106.pdf

**FTC Privacy Issues page:** http://www.ftc.gov/privacy/glbact/

**FTC Standards for Safeguarding Customer Information:** http://www.ftc.gov/os/2002/05/67fr36585.pdf

## *HIPAA*

In the healthcare industry, the security rules of the Health Insurance Portability and Accountability Act (HIPAA) require that participants in this sector, which includes healthcare insurers, providers, and clearinghouses, "must assure their customers (for example, patients, insured individuals, providers, and health plans) that the integrity, confidentiality, and availability of electronic protected health information they collect, maintain, use, or transmit is protected."

One misconception is that HIPAA applies only to healthcare providers and insurers. In reality, the inclusion of "clearinghouses" means that the act impacts some organizations that consider themselves neither healthcare providers nor insurers. Any organization that manages data for healthcare providers and insurers also falls under the act's data privacy and protection regulations.

In requiring data availability, HIPAA does not leave the definition of "availability" to the discretion of the healthcare provider. Instead, it defines it as "the property that data or information is accessible and useable upon demand by an authorized person." Thus, it is not enough to ensure that a healthcare provider can, eventually, recover data from some offsite location should it be destroyed. The provider must ensure that data is always accessible in a timely manner to the people who need it.

**Links:**

**Full act:** http://www.cms.hhs.gov/hipaa/hipaa1/content/hipaasta.pdf

**Health Insurance Reform: Security Standards:**
http://www.cms.hhs.gov/hipaa/hipaa2/regulations/security/03-3877.pdf

## *Service Level Agreements (SLAs)*

Beyond the requirements set by governments, some businesses set legally binding benchmarks for themselves. Sales contracts increasingly include Service Level Agreements (SLAs) that, because of the business' dependence on information technology, can be fulfilled only if data and applications are continuously available.

While a failure to comply with these agreements likely won't result in a jail term for corporate executives as might be the case if a law is broken, the financial penalties can be severe. Beyond any contractually imposed fines, repeated failures to comply with SLAs could irreparably damage a company's reputation and, therefore, its ability to win new business. As such, SLAs have two serious implications that can have significant effects on an organization's financial liabilities:

1. Direct Litigation: Law suits filed for breach of contract vis-à-vis the SLA.

2. Down Stream Liability:  Law suits filed by 3rd parties who have been affected by the organizations breach of the SLA.

## Consolidation

When it comes to information technology, consolidation is one of the watchwords of the day. There are at least four factors behind this movement: compliance issues, a growing concern about security, industry consolidation, and business streamlining.

With the advent of strict regulations dictating that companies secure data, protect its privacy and ensure its availability, organizations have begun to realize that the data center “glass house,” with its centralized management and control, is a better place to achieve those objectives than the departmental nooks and crannies that servers had been distributed to in the recent past. Security and control are just too difficult to define, monitor and enforce when hardware, software and data are widely distributed throughout the organization.

Industry consolidation is another driver of technology consolidation. After a few years’ lull, merger and acquisition activity appears to be increasing. Obviously, this has implications within the merged and acquired companies, but none more so than in their IT departments. To take advantage of economies of scale, systems must be merged, with the result that fewer servers become responsible for managing more of the combined businesses’ activities and value.

Business streamlining has much the same effect. In the latter two decades of the twentieth century, the trend in information technology was toward decentralization. Mainframe, and even midrange, servers were shunned for much less expensive commodity servers. However there was a problem with this approach. In many cases, it *did* reduce hardware costs, but just about every other cost increased:

- Software licenses were required for every server.
- Floor space was required for all of the servers and their peripheral devices.
- Servers typically had to be administered, backed up, and secured independently, thereby increasing administration costs.
- Skills often had to be allocated to every server and, when those servers consisted of a variety of different architectures, there was little or no room to share skill sets among them, which made the achievement of economies of scale in human resource usage impossible.
- Because servers were decentralized and, therefore, not directly under the control of the rigorously managed data center, the administration, backup and security functions were not performed with a consistent level of quality, resulting in the occasional loss of data and operation stoppages—at a significant cost to the company in the form of lost revenues and increased labor costs to recover from the loss.

Over the past few years, many organizations have recognized that the distribution of data and applications to decentralized commodity servers was a false economy and, therefore, they have been busy recentralizing processing onto fewer servers. The result is the same as for merged enterprises: fewer servers have become responsible for managing more of the combined businesses activities and value.

This consolidation, regardless of the reason for it, raises an availability concern. Now, if one of those consolidated servers becomes unavailable—whether for scheduled maintenance or an unexpected downtime event—a far greater portion of the company suffers the consequences. In the decentralized past, an unavailable server might have affected a single department or possibly even just a single activity within one department. Now, after consolidation, if a server becomes unavailable, it might stop the entire business from top to bottom, bringing revenues and profits to a halt. Therefore, protecting the availability of these centralized systems is a much higher priority than for a small, distributed server.

The bottom line is that, as a result of business, server and supply chain consolidation, the protection of system availability has become a business imperative.

## 10 Tips for High Availability (HA) Planning

Moving forward with HA planning requires consideration of many factors. The tips below will help organizations review their current HA plans, if any, and begin to make new plans when necessary.

### Tip 1: Keep Your Customers Happy

Focus on keeping your goods or services flowing to your customers. This will greatly limit the financial impact of a disaster and allow the organization to easily calculate the payback and justification of an HA solution.

### Tip 2: Be Prepared for the Short and Long Term

When a natural or man-made disaster occurs, the time to recover your primary facility could be hours, days or months. Prepare for longer-term outages by having plans that would facilitate all operations critical to customer fulfillment.

### Tip 3: Identify Critical Short- and Long-Term Application and Information Resources

In a short-term disaster, keeping clients happy may require a completely different scope of application and information resources than a long-term disaster.

### Tip 4: Understand the Impact of Industry Regulations and SLAs

From Sarbanes Oxley, to HIPAA, to GLB, to your SLAs, the protection and safeguarding of information from destruction is now regulated and/or contracted. Be sure to understand the implications of regulations, standards and contracts on your organization’s operations.

### Tip 5: Consider Consolidating Your Resources

The consolidation of information and application resources has many drivers. In addition to reducing administration and software costs, merging the applications and data that currently reside on distributed servers onto one or a few centralized servers makes it easier to ensure that integrity, security and availability protection rules are formulated and rigorously enforced for all data and applications. Another aspect of consolidation is the fusing of your high availability solutions in a way that “virtualizes” the hardware, software and data being protected. In this way, all of the HA solutions can all be monitored and managed from a single console, regardless of how many diverse platforms they might be protecting.

### Tip 6: Have Simple Plans

The simpler, the better. Plans need to be concise and straightforward. The best plans forego lengthy narratives and focus on the specific actions that staff must take to affect a recovery.

### Tip 7: Update Plans Frequently

Your HA plans should be updated frequently. You should also review any application changes to ensure that the HA configurations support any updates or modifications to the application environment.

**Tip 8: Have Contact Information for 24x7 Support**
Be sure that all staff involved in recovery have 24x7 support available from your HA solution provider, application providers and other hardware and software vendors that are part of your environment.

**Tip 9: Practice, Practice, Practice**
After installing your HA systems, devote the resources necessary to thoroughly train staff and practice typical recovery processes. Keep your staff knowledge crisp and make recovery second nature by practicing recovery procedures often.

**Tip 10: Choose Your HA Vendor Wisely**
Make sure your HA vendor is well established and has customers who have successfully survived disasters by utilizing the vendor's technology, services and methodologies. Very importantly, make sure the vendor has the resources required to provide you the support you need, when you need it. Your data and application availability—and therefore your business' continuity—depends on your HA vendor having a full range of highly available and support, and the human resources and business partners needed to back that up.

## Vision Solutions:  The Trusted Vendor for High Availability Software

The one common denominator in the compliance, consolidation and continuity trends is that they all drive a significantly enhanced need for businesses to protect the availability of their systems and data throughout the enterprise.

Vision Solutions, the only company that delivers high availability across the entire IBM eServer mid-range line—OS/400, i5/OS, Windows, Linux and AIX—through one interface, is the industry standard in eServer high availability. With more than 15 years of experience and over 2,000 accounts in more than 70 countries, Vision is listed as one of the top 300 largest software companies in the world. Over the course of its history, Vision has continued to deliver innovative solutions that lead its industry.

Beyond its own history, Vision has also hired a number of people that bring considerable breadth and depth of experience with them. For example, Vision employs more than 60 engineers with combined experience of more than 700 years. In addition, its staff of computer scientists and system architects includes three PhD holders.

As a result of its experience and innovative technologies, Vision has become the industry standard in eServer high availability, providing software, services and support solutions for managing a company's mission-critical applications and data.

Alliances are important to Vision. The company is an IBM Premier Business Partner, an IBM High Availability Business Partner, and the leading managed availability vendor for the IBM eServer iSeries (AS/400). Vision Solutions also maintains strategic alliances with industry-leading application and database companies including Misys, IBS, Intentia, Microsoft and Oracle.

Vision’s products and services, including its Visualize methodology, its ORION suite of high availability and data integration software, and its acclaimed CustomerCare program, have made Vision a leader in its markets.

Vision’s ORION suite of offerings is the industry’s first multi-platform information availability solution, designed to manage both data and application availability across an enterprise’s entire environment, all from a single view. ORION is highly scalable in supporting OS/400, Windows and Linux, as well as Oracle, Sybase, DB2/400, SQL Server and DB2/UDB.

In addition to its products and services, Vision Solutions, backed by a worldwide network of partners, provides extensive professional services, support and education to a global market. It provides a world-class Customer Care program with a 95% customer satisfaction rating.

**For More Information**

Key Information Systems, Inc.
PETE ELLIOT
Director of Marketing
1.818.737.2804
1.818.992.8970 fax
pelliot@keyinfo.com
www.keyinfo.com