

# Data Governance

## Regulatory Compliance and Business Continuity

A White Paper

*By Dennis Wenk and Christophe Bertrand*

August 2005

## *Executive Summary*

The disaster and losses of September 11 combined with recent corporate accounting scandals have created an environment in which a “Perfect Storm” of new government regulations has emerged. Organizations are now challenged to interpret a slew of new mandates and protect their key data assets—whatever the circumstances.

It is no surprise that there is a lot of confusion around these data governance issues. Do new regulations in effect pose a business continuity problem, a legal problem, or a technical question? Or do they simply require a process improvement effort? While regulatory compliance is complex, it is not necessarily complicated.

Starting with a good understanding of regulatory and business policy requirements, IT organizations can implement strategies that enhance operational efficiencies within the enterprise, lower costs, and bring organizations into regulatory compliance while understanding risk exposures and managing loss expectancy. Technologies like storage management software and storage-based virtualization can enable organizations to manage and control the rapid growth of electronic records and protect their data assets effectively.

But let’s not lose track of the “big picture.” A modern organization needs to guarantee the availability of its data and applications, the integrity of the data itself (or what good would the data be?), and its security, whether regulations demand compliance or not. Therefore, data governance is really about building compliance requirements and associated exposures into the continuity of business operations. Organizations also should recognize that building an infrastructure that ensures compliance and business continuity is a long-term process and not an overnight occurrence.

This paper examines the challenges associated with data assets, identifies and defines a few key regulations that are affecting organizations, and examines how a business-focused approach and a flexible storage infrastructure can help organizations resolve data governance issues.

# Contents

<b>Facing Today's "Perfect Storm" of Regulations .....</b>	<b>1</b>
What Keeps You Awake at Night Mr./Mrs. CFO? .....	1
Data Governance .....	1
Understanding the Value of Data .....	2
Electronic Records and Data: the Compliance Challenge .....	2
The Compliance Decision: Benefits and Risks .....	3
Common Requirements .....	4
<b>General Corporate Compliance.....</b>	<b>5</b>
Industry-specific Compliance Requirements.....	6
Where Do These Regulations Leave Us? .....	8
<b>Planning and Implementing Your Data Governance Process .....</b>	<b>8</b>
Assessing Risks .....	8
ILM/DLM or the Hyped Alphabet Soup .....	9
Managing Content and Data .....	9
Storage Management.....	9
Storage Virtualization .....	9
Business Continuity .....	10
<b>Conclusion .....</b>	<b>10</b>

# Data Governance

## Regulatory Compliance and Business Continuity

A White Paper

*By Dennis Wenk and Christophe Bertrand*

### *Facing Today's "Perfect Storm" of Regulations*

In the years following the events of September 11, substantially higher numbers of regulations regarding business continuity have been enacted than in the prior 10-year period. Thanks to the public outcry regarding the downfall of Enron and other corporations for fraudulent accounting practices, this already stormy regulatory environment has developed into a "Perfect Storm," which has brought about a slew of new government regulations and requirements. Not only are organizations expected to decipher and interpret a number of new regulations that affect their internal controls, but they are also expected to protect their key data assets—whatever the circumstances.

### What Keeps You Awake at Night Mr./Mrs. CFO?

With these new regulations come worrisome complexities and penalties: heavy fines for not complying, the prospect of jail time for executives, and the potential for auditors to refuse to certify accounts. As you ponder these, you may also be asking: "How would I close my books if my data disappears after a virus attack or a flood in my data center?" or "What about the reputation of my company?" Sarcastic minds would recommend investing in the sleeping-aid industry because today's regulatory challenges are more than enough to keep anyone up at night.

Let's face it. There is a lot of confusion around what this new regulatory environment demands. Is this a business continuity problem, or is it a legal problem? Is it a technical question or just a process improvement effort? Is a miracle tool available? While regulatory compliance is complex, it does not necessarily have to be complicated. This paper examines the challenges associated with data assets, identifies a few key regulations that are affecting organizations, and identifies how a business-focused approach and a flexible storage infrastructure might help.

### Data Governance

The real issue—the iceberg mass below the surface, not its tip—is data governance. Specifically, data governance must address areas such as operations efficiency, compliance with regulations, protection of assets, and operational resiliency. Data has become one of the most important yet intangible assets of most organizations. Actually, it is like individuals, irreplaceable if lost.

Today's regulatory environment would not have reached the intensity of a "Perfect Storm" if it were not for the seemingly uncontrollable growth of data to levels never seen before in human history. Rather than focusing on the tip of the iceberg or the symptoms associated with noncompliance, translating data governance objectives into a meaningful IT infrastructure is key in today's economy.

## Understanding the Value of Data

There is no question that data is a very valuable corporate asset. Quantifying the value of physical assets is fairly straightforward, but quantifying the value of an electronic asset such as data is difficult. Simply identifying individual point-problems, such as the costs of electronic discovery or reconciliation issues, implies a consequence but this does not define value.

Identifying exposures to data, like electronic discovery, is fundamental, but understanding the economic value of data is vital. Without knowing data's economic value it is difficult to know how to control and protect data, because without a sense of its value there is no way to evaluate potential solutions. Data value is not always obvious and, since data is one of only two irreplaceable assets, clear thinking about data is an imperative. Intuitive judgments often lead to mistakes, and mistakes about data could have dire, catastrophic consequences.

## Electronic Records and Data: the Compliance Challenge

There are currently more than 10,000 U.S. federal, state, and local laws and regulations addressing what, how, when, and why records must be created, stored, accessed, maintained, and retained over increasingly longer periods of time. Many of these regulations carry stiff penalties for failure to comply, up to and including fines and imprisonment. Compliance entails putting record retention strategies in place for both hard copy and electronic records.

Companies are struggling to ensure they are complying with record retention requirements in this ever-expanding universe of state and federal regulations. Often these regulations are written by bureaucrats with little or no understanding of current technologies for electronic document retention and management, and definitive interpretations are elusive. However, IT organizations must understand the evolving regulations and their implications for ongoing system requirements as well as their personal liability. Organizations need the involvement of their IT professionals in areas such as understanding internal control and reporting mechanisms, adjusting the IT infrastructure and controls to support financial reporting compliance requirements, identifying risks of data loss, and so forth. The list is long.

Considering the wide variety of record-keeping requirements and specified retention periods, some companies are trying to simplify policy definition and limit administrative complexity by retaining all electronic records for the longest applicable retention period. This is often a more feasible approach for electronic documents than it is for paper documents, and technical and economic trends will continue to move in that direction.

The practice of keeping data for long periods of time in a recoverable format—whether for months, years, or decades—raises a number of issues that must be understood and addressed before an electronic document retention plan is put in place. Long retention periods will drive the need for efficient storage strategies over time. A couple of key questions invariably come to mind:

- :: Do the regulations in your business or industry require a disaster recovery capability for the document archives?
- :: Even if no regulatory requirement exists for disaster recovery capability, is it a common practice in your industry, and should you implement a disaster recovery plan to meet evolving stakeholder expectations and minimize business and legal risks?

This paper's "General Corporate Compliance" section cites specific examples of laws and regulations that businesses should consider when beginning an education and assessment process regarding electronic document retention. It also summarizes the common requirements that appear in many regulations, which are aimed at preserving records and ensuring or controlling access to the records that are retained.

## The Compliance Decision: Benefits and Risks

Companies have two possible strategic paths to choose from when faced with the question of how to address regulatory compliance:

- :: They can wait and do nothing...taking their chances and betting that it won't happen to them.
- :: They can start down a path of ensuring compliance by first becoming educated on the regulations affecting them and then beginning to intelligently plan and deploy an approach that will assist in their compliance efforts.

### It's Not Just the Fines...

The path an organization chooses can have far-reaching consequences. For those organizations that choose the second path—education and intelligent deployment—the dividends can be huge. In contrast, for those organizations that choose to do nothing, the company's risk level can rise substantially in the current regulatory and legal environment. Take for example the case of Arthur Andersen just a few years ago. Andersen was caught deleting records after notice of a pending legal action. (In the legal community this is referred to as spoliation of evidence.) And what happened to Andersen? They quickly went out of business—not only due to the fines that were assessed, but also due to the negative publicity that drove current and potential customers away.

The company that chooses to ignore or knowingly violate document-retention regulations risks the wrath of customers and potentially a large hit to shareholder equity. The same reaction could result from an involuntary loss of key data. How will you explain to your customers that their account information has been wiped out due to a sprinkler malfunction in the data center, or that you can't deliver your semi-finished goods because production systems have lost their database...thus interrupting the supply chain?

In addition to purely regulatory requirements, companies must consider the document retention implications of litigation support and electronic document discovery. An increasingly common example would be an eDiscovery order issued against a company's e-mail system. The company that is served with the discovery order must produce all required messages in a timely manner, and they are responsible for the costs associated with the discovery. What's even more interesting is the question of what you would do if you lost the data in question, not because you "wanted" to, but because circumstances affected the data (corruption, disaster, etc.).

At this point you might have some of the following thoughts:

- :: "So what! Think of all the money I can save by doing nothing, if legal action is never brought against me! And disasters don't happen all the time. They actually seldom occur!"
- :: "Doesn't a company need to weigh the likelihood of potential legal action against the cost of implementing a records management system? Can't I purchase insurance to cover the cost of penalties? Why shouldn't I take my chances and just do the bare minimum to backup my data?"

To answer these questions, consider these points:

- :: **TCO and ROI.** Of course you should evaluate the total cost of ownership (TCO) of the solution over its life as well as its return on investment (ROI). The analysis should include not just reduction of potential document search and recovery costs, but also other impacts of acting—or of not acting. For example, consider possible regulatory enforcement actions and legal fines. And consider the possibility of jail time. The climate has changed over the past couple of years. The possibility of jail time is increasing.
- :: **Public Relations.** What would be the cost of negative public relations for your company now or the potential loss of future business?
- :: **Shareholder Equity.** Negative publicity can drive the company's stock price down for long periods of time. A hit to shareholder equity could affect an executive's bonus, stock options, or job tenure.

## Common Requirements

Most state and federal regulations focus on a few common requirements regarding the creation and retention of business records. The rules tend to focus on two main aspects of record-keeping practices and technology:

- :: **Retention**—what content to keep, for how long, and in what format
- :: **Security**—protection and auditability (proof of authenticity)

For data security, auditors will question how the integrity of the data is maintained, how readily available the data is and needs to be, and (in the case of privacy laws) how the confidentiality of the data is established and preserved.

Don't these requirements essentially look like what the results of a successful business continuity process should be?

Key to the implementation and ongoing success of a data governance policy is the identification and understanding of these common requirements. Another important factor for a successful long-term regulatory compliance program is the understanding that an effective solution will include both procedural and technological aspects.

Procedural aspects include creation of actual policies for record retention that are directed to employees, an education program for the employees, and an organization structure that clearly defines who is in charge of the program. However, in the case of electronic records and documents, other, more interesting aspects to consider are the technological aspects. These would include evaluation and selection of records management software (which is only one of the dimensions to consider), the crucial choice of storage platform (disk, tape, etc.), and disaster recovery capabilities—all essential infrastructure IT requirements.

Let's take a closer look at a few examples of compliance requirements that impact electronic record retention—either very broadly, or in specific industries.

## General Corporate Compliance

Some regulations span multiple industries and apply to most companies regardless of the type of business they conduct. The U.S. Sarbanes-Oxley Act of 2002 is often cited as an example, having a potentially huge financial and IT resource impact upon organizations. The Sarbanes-Oxley legislation and rule-making were a direct response to corporate accounting and reporting scandals such as Enron and WorldCom and were intended to “deter and punish corporate accounting fraud and corruption, ensure justice for wrongdoers, and protect the interests of workers and shareholders.”

For example, the Sarbanes-Oxley Act requires CEOs and CFOs of publicly traded companies to certify their financial reports and therefore the supporting data, and also to certify their “internal controls over financial reporting.”

Penalties for compliance failure include:

Behavior	Sentence
The alteration, destruction, or concealment of any records with the intent of obstructing a federal investigation	Fine and/or up to 10 years imprisonment
Failure to maintain audit or review “work papers” for at least five years	Fine and/or up to 5 years imprisonment
Anyone who “knowingly executes, or attempts to execute, a scheme” to defraud a purchaser of securities	Fine and/or up to 10 years imprisonment
Any CEO or CFO who “recklessly” violates his or her certification of the company’s financial statements	Fine of up to US\$1 million and/or up to 10 years imprisonment
If “willfully” violates	Fine of up to US\$5 million and/or up to 20 years imprisonment
Two or more persons who conspire to commit any offense against or to defraud the United States or its agencies	Fine and/or up to 10 years imprisonment
Any person who “corruptly” alters, destroys, conceals, etc., any records or documents with the intent of impairing the integrity of the record or document for use in an official proceeding	Fine and/or up to 20 years imprisonment
Mail and wire fraud	Increase from 5 to 20 years imprisonment
Violating applicable Employee Retirement Income Security Act (ERISA) provisions	Various lengths depending on violation

To verify these internal controls, auditors will need to examine records contained in enterprise resource planning (ERP) applications and reports generated by financial accounting applications along with documents that support these business processes. A properly designed record-retention system not only expedites the recall, production, and authentication of this information, but also can be leveraged to provide additional benefits for the company. These benefits can range from the ability to automatically replicate and house this data offsite to ensuring business continuity in the event of a disaster.

## Industry-specific Compliance Requirements

Industry-specific regulations include those for banks, insurance companies, securities firms, health care providers, government contractors, drug companies, and even government agencies. Some examples of these regulations are:

### NARA Part 1234

The National Archives and Records Administration (NARA) defines and manages long-term archiving requirements for federal government agencies. Electronic record-keeping systems that maintain the official file copy of agency documents on electronic media must meet the following minimum requirements:

- :: Provide a method for all authorized users of the system to retrieve desired documents, such as an indexing or text search system
- :: Provide an appropriate level of security to ensure integrity of the documents (*§ 1234.28 provides for backup and recovery of records to protect against information loss*)
- :: Provide a standard interchange format, when necessary, to permit the exchange of documents on electronic media between agency computers
- :: Provide for the disposition of the documents including, when necessary, the requirements for transferring permanent records to NARA

### FOIA

The Freedom of Information Act (FOIA) for local, state, and federal government is one regulation that puts additional strain on their resources. IT budgets and staffs within these agencies are usually already stretched to the breaking point even without the requirement to make all or part of their data available to the public on a timely basis. With this law existing as a largely unfunded mandate, the task of identifying, protecting, recovering, preserving, and presenting this data is for the most part left to local resources to fund and manage.

### HIPAA

The Health Insurance Portability and Accountability Act (HIPAA) sets national standards for electronic data interchange in the health care industry. The HIPAA regulations also address the security and privacy of health-related electronic data, with regard to its use, storage, and exchange.

The health services industry includes two major components: health insurance providers and health care providers. Health care providers, such as hospitals, must retain medical records for five years, six years, the life of the patient, or for two years after a patient's death—depending on the applicable federal and state laws and regulations. Protected health information (PHI) must be protected in compliance with the HIPAA privacy and security rules. Penalties for willful noncompliance include up to US\$250,000 in fines and up to 10 years in prison. The HIPAA Security Rule states that reasonable and appropriate administrative, physical, and technical safeguards must be maintained to ensure the confidentiality, integrity, and controlled availability of PHI. The rules also state that required data must not be altered, destroyed, or inappropriately processed.

### 21 CFR Part 11

When firms regulated by the U.S. Food and Drug Administration (FDA) generate records in electronic form, their record storage systems are subject to rules specified in the Code of Federal Regulations (CFR), Chapter 21, Part 11. In the industry, these are commonly known as 21CFR11, or the Part 11 rules.

FDA-regulated organizations include pharmaceutical companies, biotechnology firms, and medical device manufacturers. The FDA's Good Manufacturing Practices (GMP), Good Laboratory Practices (GLP), and similar rules (the GxP rules) require companies to keep records of processes that can affect product quality, safety, and effectiveness. These activities include product development, clinical testing, manufacturing, and distribution. Traditionally, companies used paper-based records to meet FDA requirements, but companies are increasingly keeping key records and documents in electronic form, and storing them in computer-based applications and storage systems.

Currently the FDA is updating its guidelines that regulate the use of electronic records and signatures. Businesses within this space will need to re-evaluate how data generated in research, clinical trials, regulatory approval, and manufacturing is maintained and preserved within the organization.

### SEC Rule 17a-3 and a-4

The Financial Services Industry in the United States consists of three main segments or types of business: securities, banking, and insurance. Each is subject to specific sets of laws and regulations. Large financial holding companies may include business units operating in all three segments and across country boundaries. Securities firms, such as broker/dealers, mutual funds, investment advisers, and transfer agents are regulated under distinct Securities and Exchange Commission (SEC) rules.

Banking firms are subject to regulations defined by the Federal Reserve, the Federal Deposit Insurance Corporation (FDIC), the Office of the Comptroller of the Currency (OCC), etc. Insurance firms are primarily regulated by the state government agencies, although federal agencies are taking a closer look at insurance industry practices under laws such as the Patriot Act.

All financial services firms are subject to the requirements of the Gramm-Leach-Bliley Act (GLBA), but there is no single enforcement agency for GLBA. Interpretation is handled by existing industry oversight authorities. For example, several banking-industry regulatory agencies collaborated to define the "Interagency Guidelines Establishing Standards for Safeguarding Customer Information" (published as 12 CFR 30, Appendix B).

Financial services firms are also subject to cross-industry regulations such as the Sarbanes-Oxley Act (US) and Data Protection Acts (EU). As mentioned earlier, the laws that control electronic documents, including e-mail, are designed to promote specific public policy goals. For example, the Securities and Exchange Act was intended to protect investors from securities-trading fraud or misleading financial reports. Regulatory agencies such as the SEC translate these legal mandates into rules and regulations. The SEC's famous "Rule 17a-4" is part of Title 17 of the Code of Federal Regulations (CFR), Section 240. The full citation is "17 CFR 240.17a-4," but the industry calls it "Rule 17a-4" for short.

The other segments of the Securities Industry are regulated under other sections of 17 CFR. The goals are similar, but the regulations for securities traders (broker-dealers) are the most specific in terms of storage requirements such as "write once, read many" (WORM) capability.

Within the financial services sector, one category of securities firm, the broker-dealer, is receiving particularly intense scrutiny from government regulators. The following section provides a closer look at SEC Rule 17a-4. Current SEC enforcement is focusing on e-mail archiving for brokers and dealers, and Rule 17a-4 imposes strong and explicit requirements for tamperproof archival storage of these required records. Some of the best-known directives within SEC Rule 17 are:

- :: Written and enforceable retention policies
- :: Storage of data on indelible, nonrewriteable media
- :: Searchable index of all stored data

- :: Readily retrievable and viewable data
- :: Storage of data offsite

## Where Do These Regulations Leave Us?

This sample of regulations, although different in origin, nature, scope, and intent can be confusing at first glance. Some tell you what to do; some tell you what not to do. Some tell you what will happen if you do something, while others tell you what will happen if you don't. None of them are particularly clear as to the single biggest question, which is how? So let's focus on the commonalities:

- :: Data must be stored
- :: Data must be secure
- :: Data integrity is required
- :: Data must be managed
- :: Data must be available when needed
- :: Offsite requirements are commonplace
- :: Processes and controls have to be in place

But there might be good news on the horizon. Most organizations are already doing something to protect their data assets. An IT infrastructure that supports the continuity of the business through advanced data protection will provide useful methodologies and mechanisms to also address today's burning corporate compliance issues.

## *Planning and Implementing Your Data Governance Process*

### Assessing Risks

While careful inquiry is important, managers need economic motivation to make rational decisions by balancing the cost of the solutions with the benefits of data governance. But market-value for data does not generally exist. Careful sorting of the economic consequences is an approach to determine data's economic value. The economic consequences translate into the aggregate loss potential, which is related to either not having, or not having access to, the data. By assessing their data's economic value managers gain a rational method with which to evaluate data governance benefits through cost-benefit balancing.

Risk assessment (which includes reviewing required regulations and other legal requirements) and policy creation are the first two steps in determining what infrastructure changes may need to be made. However, the more complex the organization is—in number of employees, geographic distribution, and number of regulations—the more dramatic the infrastructure changes that may be needed.

With the end goal being to effectively protect data and automate and secure management and placement, organizations may find that the most critical technologies they need to deploy include one or more vendor-specific technologies. One question to ask is, "Should I wait for more vendor-agnostic solutions to emerge?" The answer to this question is...don't wait. Start the risk assessment and policy creation now.

## ILM/DLM or the Hyped Alphabet Soup

With all the recent hype around information lifecycle management (ILM) or data lifecycle management (DLM), many vendors have tried unsuccessfully to position themselves as “information” companies. This leaves potential customers on their own to resolve their biggest challenge: how to manage and optimize their IT storage infrastructure to meet the myriad of compliance and other IT data governance needs.

Aligning IT and business objectives is not just about managing data through its lifecycle. It’s about IT understanding the needs of the business and building, managing, and adapting a storage infrastructure to optimize data delivery in support of the myriad needs of the applications businesses rely upon.

To address this complex problem, the design point is really to focus on solutions that are based upon an integrated framework of hardware and software services, including application, content, data, and storage services.

## Managing Content and Data

*Content services* represent any applications that provide the ability to index, store, search, and retrieve information. Typically, this includes databases, messaging applications, file systems, ERP, customer relationship management (CRM), and unstructured content. Organizations run a wide variety of content-rich applications in support of their business processes, and these applications have diverse structured and unstructured data storage requirements. Understanding the storage requirements of these myriad data types is critical, and mastering the unique requirements of these applications can be a complex process, which will require close collaboration with leading application vendors.

Also key to data management is the ability for customers to leverage a single set of *data services* for all their migration, replication, backup, and security needs. Based upon an understanding of application storage requirements, storage cost, performance, functionality, and availability can be optimized using comprehensive data management tools for backup, migration, replication, and security.

## Storage Management

Many enterprises are unable to quantify how large their storage infrastructure is, how well its resources are utilized, who is using them, and how they are using them. Storage management software can enable organizations to inventory and quantify what they have, where it is at, and who owns it. For this software to be effective, it needs to be easy to deploy, simple to manage, and relatively inexpensive to license. These applications should also offer more advanced capabilities, such as automated provisioning and storage pooling, that are managed from a central management console.

## Storage Virtualization

Storage virtualization technology promises to enable organizations to manage and control all storage resources from a central console. It can become a key capability for effective ILM. When storage management applications are used in conjunction with an ILM strategy, the placement of data based on changing value can be handled transparently and automatically based on defined record-retention policies and access requirements.

Additional enhancements are needed to support the larger storage pools associated with DLM and utility storage solutions. This has fueled a demand for a lower-cost modular storage tier to be used for reference data, for business continuity data that no longer requires high-speed, nonstop availability but must still be retained, and for business intelligence and compliance applications.

However, low cost alone is not enough to satisfy compliance. Compliance requires data protection with snapshots and mirrors. It requires business continuity processes with distance replication. It demands online migration for replacement of aging hardware technology and depends upon features to ensure data integrity and privacy.

## Business Continuity

Many technology-based business continuity options are available today, ranging from traditional data protection based on tape backups, to more sophisticated infrastructures that rely on the combination of replication technology, clustering, and long-distance networks. As mentioned earlier in this paper, there is a clear business requirement to understand data protection in economic terms, using risk analysis, for example, or other methodologies like business impact analysis. Part of the determination process will involve understanding regulatory burdens placed on the organization. Because all data is not born equal, a continuum of data protection techniques can be mapped to the relative importance of data.

The perfect picture is one in which the infrastructure is derived from the analysis, leveraging the most appropriate and effective technologies. Some data may require snapshots and local clones for management questions, some data must be available out of region and immediately recoverable, and other data may need protection but may be a good candidate for tape if a longer recovery time is acceptable. Local replication, long-distance replication, and optimized backups that leverage disk infrastructures, for example, are all underlying technologies that support the effort, and all should therefore be considered.

## Conclusion

Today's technologies now enable organizations to begin building an infrastructure that will meet the most stringent regulatory requirements and protect critical data assets. Starting with a good understanding of regulatory and business policy requirements, IT organizations can implement strategies that enhance operational efficiencies within the enterprise, lower costs, and bring organizations into regulatory compliance while understanding risk exposures and managing loss expectancy. And technologies like storage management software and storage-based virtualization can enable organizations to manage and control the rapid growth of electronic records and protect their data assets effectively.

Hitachi Data Systems can help organizations construct a strong and compliant approach to data governance with Application Optimized Storage™ solutions. Built upon a common framework of comprehensive storage, data, content, and application services, Application Optimized Storage solutions provide the appropriate infrastructure, management, and data delivery to optimize storage for diverse application and data protection requirements. Benefits to strong data protection include lower regulatory and legal risks and costs, better information availability, and employee productivity—and increased confidence of customers and investors in the company's ability to survive and respond to the challenges of the electronic information age.

 **Hitachi Data Systems Corporation****Corporate Headquarters**

750 Central Expressway  
Santa Clara, California 95050-2627  
U.S.A.  
Phone: 1 408 970 1000  
**www.hds.com**  
**info@hds.com**

**Asia Pacific and Americas**

750 Central Expressway  
Santa Clara, California 95050-2627  
U.S.A.  
Phone: 1 408 970 1000  
**info@hds.com**

**Europe Headquarters**

Sefton Park  
Stoke Poges  
Buckinghamshire SL2 4HD  
United Kingdom  
Phone: + 44 (0)1753 618000  
**info.eu@hds.com**

Hitachi Data Systems is registered with the U.S. Patent and Trademark Office as a trademark and service mark of Hitachi, Ltd. The Hitachi Data Systems logotype is a trademark and service mark of Hitachi, Ltd.

Application Optimized Storage is a trademark of Hitachi Data Systems Corporation.

All other company names are, or may be, trademarks or service marks of their respective owners.

Notice: This document is for informational purposes only, and does not set forth any warranty, express or implied, concerning any equipment or service offered or to be offered by Hitachi Data Systems. This document describes some capabilities that are conditioned on a maintenance contract with Hitachi Data Systems being in effect, and that may be configuration-dependent, and features that may not be currently available. Contact your local Hitachi Data Systems sales office for information on feature and product availability.

Hitachi Data Systems sells and licenses its products subject to certain terms and conditions, including limited warranties. To see a copy of these terms and conditions prior to purchase or license, please go to [http://www.hds.com/products\\_services/support/warranty.html](http://www.hds.com/products_services/support/warranty.html) or call your local sales representative to obtain a printed copy. If you purchase or license the product, you are deemed to have accepted these terms and conditions.

©2005, Hitachi Data Systems Corporation. All Rights Reserved.

WHP-199-00 August 2005