

How Application Optimized
Storage™ Solutions from
Hitachi Data Systems Help
Companies Achieve
Regulatory Compliance

A White Paper

By John Harker and Carlos Soares

January 2006

Executive Summary

Regulatory compliance has put the storage industry front and center as a means of insuring enterprises against corporate risk. Storage often becomes one of the major cost areas in compliance projects, with auditing practices, networking, and application software being other major cost areas. Many regulations already affect data storage infrastructure and practices, and the list can be expected to grow longer. On July 30, 2002, Congress passed the Sarbanes-Oxley (SOX) Act, which requires all public companies to preserve original and verified copies of data related to audits by their accounting firms for seven years. Even though SOX focuses on data and information related to auditing firms, in practical terms it applies to the enterprise itself, due to the inextricable links among accounting, auditors, and IT. In addition to SOX, there are many industry-specific compliance regulations concerning storage. These regulations generally require the establishment of reliable electronic records management (ERM) systems and set goals for business continuity planning, including backup and recovery for the entire enterprise.

Application Optimized Storage™ solutions from Hitachi Data Systems help customers minimize the time and cost of achieving compliance when used in conjunction with sound accounting systems, data archives, and ERM systems. As is typical in storage compliance investment analysis, both compliance- and non-compliance-related benefits occur. This paper analyzes storage compliance requirements, maps the requirements to Hitachi products and solutions, and presents a case study illustrating the use of the Hitachi HiReturn™ investment analysis program.¹

¹ The HiReturn tool is vendor-neutral and calculates return by using either the total cost of ownership or internal discounted return on investment method.

Contents

| | |
|--|-----------|
| Introduction to Storage Industry Regulatory Compliance..... | 1 |
| Application Optimized Storage Solutions Help the Enterprise Achieve Regulatory Compliance | 4 |
| A Tiered Storage Infrastructure Has Benefits beyond Regulatory Compliance..... | 5 |
| An Enterprise Record Archive Can Help with SOX Compliance and Result in Data Mining Benefits..... | 6 |
| Two Accepted Frameworks for IT Systems' SOX Compliance..... | 6 |
| Implementing a Tiered Storage Architecture for Compliance | 9 |
| Five Steps for Matching Specific Application Optimized Storage Solutions to Specific Industry Regulations | 12 |
| Step 1. Assess Risks and Costs | 12 |
| Step 2. Understand the Products and Solutions Available to Support Your Compliance Efforts | 13 |
| Step 3. "Short-list" Available Solutions and Services for Implementation..... | 20 |
| Step 4. Determine ROI | 20 |
| Step 5. Implement Auditing and Monitoring | 20 |
| The Benefits of Using Application Optimized Storage Solutions for Compliance | 21 |
| Customer Case Study..... | 21 |
| Reduced Cost and Time to Achieve Compliance..... | 25 |
| Benefits of Infrastructure Simplification Solutions | 25 |
| Benefits of the Business Continuity/Disaster Recovery Solutions..... | 25 |
| Appendix A: Acronyms | 26 |
| Appendix B: Storage Regulations Affect All Industries | 28 |
| Sarbanes-Oxley | 28 |
| Storage Regulations Affecting the Health Care Industry..... | 29 |
| Storage Regulations Affecting the Financial Services Industry..... | 30 |
| Storage Regulations Affecting Government Agencies..... | 32 |
| Storage Regulations Affecting Public Utilities | 34 |
| Appendix C: Description and Summary Benefits of the Infrastructure Simplification Solutions | 35 |
| Appendix D: Description and Summary Benefits of Business Continuity/ Disaster Recovery Solutions..... | 37 |

How Application Optimized Storage™ Solutions from Hitachi Data Systems Help Companies Achieve Regulatory Compliance

By John Harker and Carlos Soares

Introduction to Storage Industry Regulatory Compliance

Because each IT department is closely linked to each functional area of business, a single regulatory compliance requirement on a single business function can have a major impact on the software, hardware, networking, operations, and storage department within IT. This can lead to exploding complexity, because *multiple business functions* are typically impacted by *multiple regulatory requirements*. The Enterprise Strategy Group, a leading industry analyst firm, estimates that there are 10,000 or more federal, state, and local laws and regulations in the United States alone. Around the world, new regulations are continuously evolving that demand data accountability, reliable records management systems, archiving of unaltered documents and messages, and reliable business-continuity and disaster-recovery systems and practices. These mandates apply not only to governments but also to private entities and affect all major industries. The storage regulations affecting major industries are described in Appendix B, which can be used as a guideline for enterprises seeking to determine which regulations affect their IT operations.

Compliance involves keeping data not only fully intact and secure but also easily retrievable at any time for long durations. A commonality of most of these laws and regulations is that they address the process by which records must be created, stored, accessed, maintained, and retained while keeping them secure and private over long periods of time. But without specifics about how this is to be accomplished, the regulations mostly call for sound storage policies, processes, infrastructure, and management practices with set goals. Striving for storage excellence, therefore, is a common sense way to meet the goals set by the regulations and laws.

As Table 1 shows, most regulations carry penalties for noncompliance that include fines and other punishments, with the most severe being imprisonment of executives. As a result of the penalties, enterprise personnel at all levels have an extra incentive to pursue sound IT management systems and practices. Although the compliance incentive is largely negative, compliance projects should be viewed as a positive opportunity to pursue new business value through IT initiatives that often pay for themselves in terms of operational savings alone before compliance benefits are even factored in.

Table1. Summary of Current Laws and Regulations Affecting IT Storage Infrastructure and Practices

| Law or Regulatory Body | Storage-related Sections | Storage Requirements | Penalties |
|---|---|---|---|
| BASEL II | Basel II Accord of 2004 | Requires business continuity and disaster recovery plans to ensure continued operation in the event of a disaster and thereby limit losses | Fines and other penalties |
| CFTC (U.S. Commodity Futures Trading Commission) | 17 CFR Part 1 amendment to CFTC Regulation 1.31 | Requires a reliable records system to store electronic data for 5 years | Fines and other penalties |
| U.S. Department of Defense (DoD) | DoD 5015.2 | Requires records management based on NARA, including safeguards against disaster | DoD records management program Lost contracts, disallowed cost recovery |
| FDA (U.S. Food and Drug Administration) | 21 CFR Part 11 | Requires common portable formats for electronic information and signatures to preserve original content and meaning for 2 years (food), 3 years (drugs), or 5 years (biologics*) for manufacturing, processing, and packing Requires certain companies to keep records of processes that can affect product quality, safety, and effectiveness | Fines and other penalties |
| FERC (Federal Energy Regulatory Commission) | FERC Rules RM01-12-00 (Appendix G) | Sets retention periods for public utilities and requires protection from disaster | Fines and other penalties |
| GASB (Governmental Accounting Standards Board) | Statement No. 34, June 1999 | Requires a business continuity plan for all agencies operating a utility, so that their mission can continue during a crisis or disaster | Fines and other penalties |
| GLBA (Gramm-Leach-Bliley Act) | "Safeguards Rule" 16 CFR Part 314 | Requires financial institutions to have technical structures to protect the privacy and integrity of personal consumer information | Fines and up to 5 years in prison |
| HIPAA (Health Insurance Portability and Accountability Act) | Sec 1173(d)(2) | Requires medical records data to be maintained for 6 years, or 2 years after a patient's death | US\$250,000 and up to 10 years in prison |

* **Biologics** refers to a new class of immunosuppressant drugs only recently being approved by the FDA for rheumatoid arthritis. Biologics are also used for psoriasis and experimentation is under way for other skin disorders.

Table 1. Summary of Current Laws and Regulations Affecting IT Storage Infrastructure and Practices *(Continued)*

| Law or Regulatory Body | Storage-related Sections | Storage Requirements | Penalties |
|---|---|--|--|
| NARA (National Archives and Records Administration) | NARA Part 1234 | Requires reliable records systems for all federal agencies, including access, retrieval, indexing, portability, backup and recovery, and archiving | Requirements for all government agency clients of NARA Noncompliance penalties are not statutory but can result in loss of funding, lack of promotion, etc. |
| NASD (National Association of Securities Dealers) | NASD 3010 and 3110 | Requires supervision of client communications, including e-mails (NASD 3010) Requires retention of correspondence and data to meet SEC Rule 17a-4 (NASD 3011) | Fines and other penalties |
| NERC (North American Electric Reliability Council) | Rule 1200 (1216.1) | Mandates disaster recovery plans by the end of 2005 for electricity companies | Fines and other penalties |
| NYSE (New York Stock Exchange) | Rule 440 | Requires broker-dealers to make and preserve records per SEC Rule 17a-3 and 17a-4 | Fines and other penalties |
| Other rules governing government agencies | 800-34, 800-53, COG, COOP, FISMA, FOIA, and NIST | Using differing language, these rules require sound data security, backup and recovery, business continuity planning, and disaster recovery for government agencies and contractors | Government sanctions |
| SOX (Sarbanes-Oxley Act) | Sections 301, 302, 802(a), 802(a)(1), 802(a)(2) Regulations S-X, Rule 2-06 | Requires all audit and review information to be retained for 7 years. | Fines and up to 20 years in prison |
| SEC (U.S. Securities and Exchange Commission) | 17a-3, 17a-4, 17ad-6, and 17ad-7 | Requires firms to “make” records (17a-3) Requires storage and retrieval of records on WORM storage (17a-4) Requires storage mechanisms to ensure accessibility, security, and integrity of records (17ad-6) Requires “means to recover data” (17ad-7) | Fines up to US\$500 million and other penalties |

Although the language of the laws and regulations varies widely and specifics are left intentionally vague by regulators and legislators, the laws all reflect governments' increasing tendency to require reliable records storage systems and sound storage management practices across the entire spectrum of industry and government. In view of this ever-evolving set of laws, Application Optimized Storage™ solutions from Hitachi Data Systems (consisting of hardware, software, and services) can help compliance teams achieve compliance, both now and in the future.

Application Optimized Storage Solutions Help the Enterprise Achieve Regulatory Compliance

The Application Optimized Storage solutions are a synergistic integration of products and services. Take the Hitachi Message Archive for Compliance solution, an integration of Hitachi Data Retention Utility software with Hitachi midrange ATA-based storage systems and implementation services. This solution can be used to create large, economical storage archives that deliver terabytes of secure online capacity for readily accessible unaltered data in the event of an audit. Online archives can be supplemented and maintained at a total cost of ownership (TCO) that is often less than or equivalent to that of tape when the labor-intensive costs of tape operation are offset by incremental capital expenditure in storage. The Data Retention Utility is also ideal for building electronic records management (ERM) systems when combined with effective ERM application software. A sound ERM system can directly meet SOX and other compliance requirements. Although the specifications for such an ERM system are left open in many regulations, Hitachi Data Systems and others find that DoD 5015.2 is a solid best-practices ERM specification from which to start planning, and this paper discusses this specification in some detail. More than just a collection of products and services, Application Optimized Storage solutions are based on a comprehensive tiered storage infrastructure framework that provides automated, policy-based matching of application requirements and the IT infrastructure throughout the data lifecycle.

Application Optimized Storage solutions address both operational efficiency and business continuity. The Hitachi Data Systems infrastructure simplification solutions focus on operational efficiency and reduce both capital expenditures (CapEx) and operating expenditures (OpEx) through consolidation, aggregation, tiering, data lifecycle management (DLM), and secure data partitioning. *Aggregation* refers to the unique ability of Hitachi TagmaStore™ Universal Storage Platform and Network Storage Controller to function as both enterprise-class storage and a network storage controller, allowing central management and data migration of all the data in your enterprise. This solution enables effective DLM, which is sometimes called information lifecycle management (ILM). Both *DLM* and *ILM* refer to the management of data throughout its entire lifecycle, from creation through operational use to archiving and eventual deletion.

Many regulations set requirements for business continuity planning and the ability to restore operations and services quickly in the event of a disaster such as a hurricane, earthquake, tsunami, or terrorist attack. The Hitachi business continuity/disaster recovery products include enhanced backup and recovery solutions for both open systems and mainframe environments that the competition just can't match. Known for decades as the industry leader for the highest-availability storage products, Hitachi Data Systems provides business continuity solutions that offer unsurpassed technical excellence in disaster prevention and planning as well as backup and recovery. Hitachi disaster prevention, planning, and recovery solutions are the industry's most advanced and will result in both hard and soft CapEx savings and hard and soft OpEx savings for the enterprise.

Hitachi Data Systems encourages you to place these Application Optimized Storage solutions on your short list of tools that facilitate regulatory compliance. Note that a complete regulatory compliance plan involves many dimensions, technologies, and areas of expertise—including legal advice not available from Hitachi Data Systems. Hitachi tools provide a good storage foundation for overall compliance and therefore serve an important role.

When evaluating and implementing storage infrastructure changes for your business, it is important to take a comprehensive “big picture” approach and bring together the best IT systems, software, and practices to achieve not only compliance but also business value. Application Optimized Storage solutions are designed to leverage your current storage investments while better aligning them for future growth and facilitating regulatory compliance audits. These solutions are tightly integrated through the Hitachi HiCommand® storage management software and use the unique and proven Hitachi approach to storage virtualization.

Because Hitachi solutions often pay for themselves in terms of business value alone, it is often not necessary to put an “expected value” of the benefit of “avoiding fines and other sanctions” into your return-on-investment (ROI) calculations. Because of its thorough yet flexible approach, the Hitachi HiReturn™ investment analysis program/tool can leave your economic decision makers with an understanding that they should be making investments in a tiered storage architecture in any case and that the big picture involves more than just meeting today’s regulatory storage requirements. This approach should also assuage any concerns your management may have about “vendor lock-in,” because the HiReturn investment analysis tool is vendor-neutral and incorporates all the major storage on your floor. Hitachi Data Systems believes that “best storage practices” always make sense from both an economic and regulatory point of view and for both today’s and tomorrow’s optimization of your compliance plan within a big-picture context of solid business value.

A Tiered Storage Infrastructure Has Benefits beyond Regulatory Compliance

The recent trends of exploding growth in corporate data and the increasing number of government regulations affecting storage can lead to ongoing frustration in storage infrastructure design and management. As with all IT problems, the best approach is always to preplan intelligent policy and strategy and then execute them systematically. Many analysts agree that adopting a DLM storage strategy such as the Application Optimized Storage solution framework and building this strategy on a sound tiered networked storage architecture that meets compliance requirements while sensibly managing data growth is a sound policy. If you have not implemented a tiered architecture, perhaps now is an auspicious time to do so. What used to be known as “best IT practices” for storage infrastructure and management is slowly being defined as requirements by laws and regulations. The benefits of a tiered storage infrastructure always go beyond compliance and help increase the operational efficiency and business continuity of the enterprise itself. Compliance benefits, therefore, should be only one set of factors in storage investment analysis.

Analyzing the regulations in Table 1 reveals that the regulations differ in terms of language, origin, nature, scope, and intent. This can be confusing at first glance, because some tell you what to do and some tell you what not to do. None of them are particularly clear about how to meet the requirements. However, the regulations have certain commonalities, which is a good place to start in designing your storage compliance planning and implementation process.

- :: 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.

Compliance is not a brand-new topic; most organizations are already doing something to protect their data assets, ensure business continuity, lower TCO, and design storage infrastructures requiring simpler administration. But a tiered storage architecture can generate fresh operational, business continuity, and disaster recovery cost savings and also provide protection against litigation. Application Optimized Storage solutions are supported by a five-step process to achieve both types of benefits, as shown later in this paper. The Hitachi compliance support process uses a strategy that reduces both risk and cost. This process demonstrates that an intelligently planned storage strategy should always be justified by total business value and not driven solely by compliance requirements. Investment analysis based on total business value is always the best perspective.

An Enterprise Record Archive Can Help with SOX Compliance and Result in Data Mining Benefits

Although Sarbanes-Oxley defines clear rules for storing corporate records, it does not specify the exact manner in which records are to be stored. Many analysts believe that the biggest risk related to ERM is the cost of retrieving data related to legal discovery. Even if all data, including e-mail messages, is backed up to tape regularly, the cost of restoring hundreds of tapes and searching millions of e-mail records can be staggering. For these reasons, many compliance efforts address setting up an enterprise data archive to not only save costs in legal discovery but also unlock information value through enhanced corporate data mining. With a tiered architecture such as that provided by Application Optimized Storage solutions, backup data can be cost-effectively stored on disk. Although Hitachi backup and archive solutions can often be justified solely on the basis of operational savings related to tape backup, SOX provides yet another point of justification. By treating SOX as a partial justification of records archiving, you can trade off human operational costs for capital investment in a cost-effective tiered storage solution for an operational efficiency solution.

Two Accepted Frameworks for IT Systems' SOX Compliance

Compliance officers, auditors, and IT organizations can use two commonly accepted frameworks for assessing SOX requirements from an IT systems view. COSO (Committee of Sponsoring Organizations) and COBIT (Control Objectives for Information and related Technology) can help CIOs translate SOX into an actionable plan for compliance, and Application Optimized Storage solutions and other Hitachi products support both frameworks.

COSO

COSO is a framework that is widely accepted by both the SEC and the U.S. Public Company Accounting Oversight Board (PCAOB) for interpreting and implementing SOX legislation. COSO specifies a series of “general computer controls,” a long list of internal controls related to IT processes in corporate data centers, including the responsibilities and systems of IT data storage managers. The quality of these storage-related IT systems can greatly influence the perception of SOX auditors regarding the accuracy and effectiveness of enterprise financial reporting. In essence, a necessary step in providing accurate financial reports is to start with accurate financial data that is created and maintained in a world-class storage infrastructure. For more information on COSO, see <http://www.coso.org>.

COBIT

COBIT is increasingly accepted internationally as good practice for control over information, IT, and related risks.² It provides a reference framework for management, users, IS auditors, and security managers. Issued by the IT Governance Institute, COBIT assists an enterprise in implementing effective data governance over the IT function throughout the enterprise.

Mapping COSO and COBIT to Hitachi Data Systems Solutions

Whatever compliance framework your company chooses, products and Application Optimized Storage solutions from Hitachi Data Systems are useful tools that help you minimize the time and cost of achieving compliance. The storage tools must be used in conjunction with sound accounting, data archiving, and ERM systems/software.

Table 2 shows the relationship of tools from Hitachi Data Systems, COBIT, and COSO.

Table 2. Application Optimized Storage Solutions Support COSO and COBIT Frameworks for Assessing IT Systems and Controls

| COBIT Characteristic | COSO Requirement | Tools from Hitachi Data Systems |
|--------------------------|---|---|
| IT strategic planning | Control environment and set clear corporate goals | HiReturn™ investment analysis program/tool |
| Risk assessment | Do risk assessment and manage internal and external risks | Risk Analysis Workshop |
| Quality management | Handle control activities—the defined policies, procedures, and practices for achieving business objectives and addressing risk | Business continuity and disaster recovery solutions |
| Service-level management | | Solutions and services |
| Performance management | Information and communication—ensuring information required for control activities is appropriate, accurate, current, and available | Many tools and solutions |
| Capacity management | | |
| Problem management | | Automatic reporting |
| Data management | | Hitachi HiCommand® Suite |
| Monitoring and reporting | Monitoring—overseeing and assessing the entire control operation | HiCommand Suite |

² See also <http://www.isaca.org>.

Looking to the Future beyond SOX

Many observers think of SOX as a harbinger of more and more regulation that will eventually result in the requirement to certify the storage infrastructure itself and eventually require the automation of more and more processes. This will almost certainly mean that an enterprise will need to install best practices and best-of-breed storage infrastructures such as the Application Optimized Storage solutions framework. John Webster, Senior Analyst and Partner of Data Mobility Group, sees this and other requirements for enterprises as he projects the trends evidenced in SOX and other regulations into the future³:

"We believe that Sarbanes-Oxley will have significant long-term effects on the storage industry. Here, we summarize our analysis of the impact of new financial reporting requirements on enterprise storage environments and those who manage them.

- :: Massive scalability of supporting storage subsystems will be required, particularly by large enterprises with high financial transaction volumes.*
- :: Automated capture and storage of financial data will be required.*
- :: Certification of storage infrastructures as capable of complying with the new regulations will become critical.*
- :: Enterprises will find it difficult if not impossible to "walk" data stored electronically in unaltered form through changes in storage media, storage devices, applications software, and operating systems.*
- :: Communication between IT management and senior executives with regard to corporate policy will become more vital, and policy-based storage management applications will become more of a "must have."*
- :: Reporting requirements will force tighter integration of mainframe and open systems data stores."*

³ Webster, John, "Of Sarbanes, Oxley and Storage – Research Perspective" (Data Mobility Group, January 8, 2003).

Implementing a Tiered Storage Architecture for Compliance

Because storage is a key part of any compliance project, compliance is not possible without a strong underlying storage infrastructure combined with best IT practices. Although much has been written about processes through which IT can establish a tiered architecture to facilitate compliance, the process is essentially common sense and probably something you are already doing.

1. Define business requirements in terms of data classes for different types of corporate information. Data classes should be defined in terms of service-level objectives such as capacity, performance, availability, and special requirements such as “write once, read many” (WORM) data. Data classes are usually assigned to an application or to data sets within applications.
2. Map data classes onto storage tiers that meet the service-level objectives of the data class. It is not uncommon for an organization to have 10 to 15 data classes mapped to three or four tiers of storage.
3. Ensure that the local and long-distance storage networks and infrastructure support the migration policies of the data classes among the storage tiers over the information lifecycle.⁴
4. Planning and implementation should support automated or nearly automated data migration for each data class or specified data sets to and from predesignated storage tiers at the appropriate time of its information lifecycle. If any extra effort is required to implement effective tier migration, it is making sure that a preplanned data lifecycle begins at the time of data creation.

The Application Optimized Storage solution framework first defines numerically ordered business requirements (most to least important), and corresponding data classes and storage tiers based on and the service-level objectives of each application. Such a rank ordering of application and data importance is unique to each enterprise and based on predetermined policies that are arrived at by discussions between IT and business managers. Some enterprises may choose to have only a few levels of Application Optimized Storage and others many. The data priority assignment process then establishes storage tiers and a migration plan to govern the flow of data sets among predesignated storage tiers throughout the data lifecycle.

How does this actually work in the real world? How are application priorities, data classes, storage tiering, and the DLM/ILM of the Application Optimized Storage solution architecture all brought together? Table 3 shows a hypothetical enterprise that determined 1...10 (importance rank ordered) applications, relating to 1...10 corresponding data classes and 1...10 corresponding storage tiers. In other words, the most important applications serving the most critical business requirements were assigned to data class #1 and storage tier #1 for this hypothetical enterprise, and so forth. Hitachi Data Systems believes that the process of matching of data classes to storage tiers with tier migration policies to meet predetermined business requirements is fundamental to aligning IT with business requirements. Hitachi Data Systems encourages you to use this example to map your own storage environment and adjust data classes, storage tiers, and migration policies accordingly.

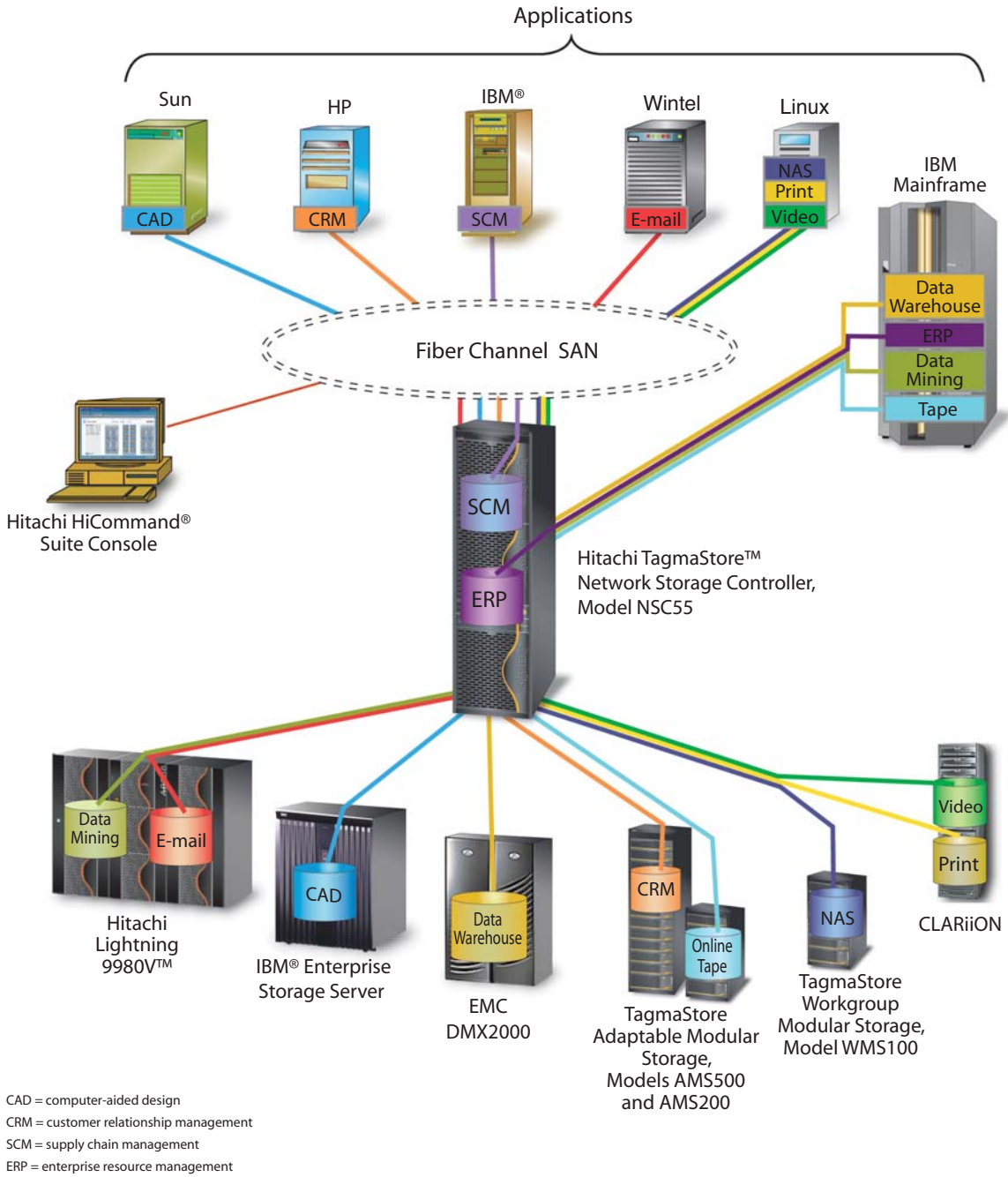
⁴ To some readers the meanings of DLM and ILM are a matter of semantics. Some use the terms interchangeably and others define ILM to be a superset of DLM, pointing out that ILM refers to the *contextual meaning of information* and that *information* as used in ILM is *data* (as used in DLM) *with context*.

Table 3. Matching 10 "Application Priorities" Based on Business Requirements to 10 Corresponding "Data Classes," and to 10 Corresponding "Storage Tiers" for a Hypothetical Enterprise.

| Storage Tier | Business Requirement | | | Data Class | Tier Migration Policy | Hitachi Storage Tiers | Hitachi Support | |
|--------------|---------------------------------------|---|--|-------------------------|-----------------------|---|-----------------|-----------|
| | Data Type | Backup Tier(s) | Business Continuity/ Disaster Recovery Tier(s) | | | | Open Systems | Mainframe |
| 1. | All SOX data | 7, 8, 9 | 10 | SOX | Tier 4 @ 120 days | Hitachi TagmaStore™ Universal Storage Platform or Network Storage Controller | Yes | Yes |
| 2. | Regulated e-mail and messages | 7, 9 | 10 | Regulated e-mail | Tier 4 @ 20 days | Hitachi Lightning 9900™ V Series enterprise storage systems | Yes | Yes |
| 3. | Other e-mail and messages | No | No | Other e-mail | Tier 8 @ 20 days | Lightning 9900 V Series systems | Yes | Yes |
| 4. | CAD, CRM, data warehouse, data mining | 8, 9 | 10 | High | Tier 8 @ 120 days | EMC, IBM enterprise storage systems, Hitachi TagmaStore Adaptable Modular Storage systems | Yes | Yes* |
| 1. | NAS | 7 | 10 | Medium | | Hitachi TagmaStore Workgroup Modular Storage systems | Yes | |
| 5. | Video, print | 8 | No | Low | Tier 9 @ 45 days | Third-party midrange systems | Yes | No |
| 6. | Priority online backup/archive | 8, 9 | 10 | Priority online archive | Tier 9 @ 180 days | Adaptable Modular Storage with SATA Intermix Option and Hitachi Data Retention Utility | Yes | Yes |
| 7. | Other online backup/archive | 9 | 10 | Online tape | Tier 9 @ 180 days | Workgroup Modular Storage systems with SATA | Yes | No |
| 8. | Tape backup | Offsite | Offsite | Tape | | Tape | Yes | Yes |
| 9. | Remote site | Remote sites mirror the storage tiers and migration policies of the primary site. | | | | | | |

* Mainframe workloads can be placed on Adaptable Modular Storage systems or Workgroup Modular Storage systems only when they are attached to a Universal Storage Platform or a Network Storage Controller.

Figure 1. Application Optimized Storage Solutions Match Data Classes to Storage Tiers Throughout the Information Lifecycle



Application Optimized Storage solutions match data classes to storage tiers with tier-migration policies to meet predetermined business requirements.

Five Steps for Matching Specific Application Optimized Storage Solutions to Specific Industry Regulations

Step 1. Assess Risks and Costs

Determine Which Regulations Require Compliance and What Actions Are Necessary

To reduce the costs, time, and distraction of storage regulations, compliance teams and officers should, as a first step, assess which regulations are pertinent, either explicitly or implicitly, now or in the future. As with all IT projects, it's wise to take a business value approach and factor in preventive measures when possible. In this way, you can benefit significantly down the road, avoiding potential audits by showing auditors a solid plan and operational practices. This approach can therefore avoid the cost and management distraction of discovery or make discovery easy to conduct if it cannot be avoided. Tables 1 through 3 can help point your compliance team to storage policies and procedures that should be implemented and followed in this respect.

Most storage regulations focus primarily on ILM issues such as ERM systems, backup and recovery systems, and business continuity/disaster recovery systems. Although it is allowable to have different policies and procedures for different IT systems under SOX and other regulations, practicality and IT efficiency always point to the wisdom of implementing common policies and practices across the global enterprise.

Establish Clear DLM, Backup and Recovery, and Business Continuity/Disaster Recovery Policies as a Preventive Measure

The best protection against future litigation is to have sound written policies and an audit trail, so these policies can be clearly followed by employees who have been trained in the policies and procedures. Compliance reviews and audits should use these policies and procedures to ensure compliance.

The Importance of a Clear DLM Policy

The U.S. Supreme Court on May 31, 2005, clarified the document-retention burden for all enterprises when it overturned the conviction of the Arthur Andersen accounting firm for destroying documents in the Enron case in late 2001. Andersen argued that its employees were following the company document retention policy in shredding tons of documents and that there was no intent to violate Section 802 of the Sarbanes-Oxley Act. The conviction was overturned on appeal because the jury had been given flawed instructions regarding this point.

The lesson to be learned here is that the intent of Congress with SOX was not to require the retention of all documents and alter a firm's DLM policy but only to require the retention of information necessary for compliance with SOX. An example of the effectiveness of having a clear DLM policy is that all major public e-mail services providers (such as AOL, Yahoo, and Excite) have clearly implemented policies of preserving communications for only a set (and usually short) period of time. Imagine the expense these providers save in not having to provide documents in a multitude of cases that would otherwise force production of these records in discovery.

The Importance of a Clear Backup and Recovery Data Management Policy

A good backup and recovery policy should define clearly what records must be kept by law or regulation for all geographies in which the enterprise operates. A company can accomplish this by using a good ERM application and directing data as required to nonvolatile unalterable media for storage according to a predefined business schedule when necessary.

The Importance of a Clear Business Continuity/Disaster Recovery Policy

Requirements for disaster prevention and disaster recovery are defined by regulation for an ever-increasing number of industries, as shown in Table 2. Today, these include many sectors of finance and government but can be expected to expand to communications companies. An example of ongoing regulation is the FCC's recent establishment of a task force to study business continuity and disaster recovery following Hurricane Katrina and the slow response of communications companies in restoring service. As government at various levels comes to consider more and more industries essential in times of disaster, a sound business continuity and disaster recovery policy is highly advisable as both a preventive measure against compliance violations and an IT best practice to ensure business continuance.

Aligning Compliance Investments with Risks Can Be Difficult

Assessing compliance risks is sometimes a difficult initial task in a compliance project. The costs and risks are often difficult to estimate and frame to executive management, with whom the ultimate decision lies. Initial cost estimates are sometimes high for a compliance project, especially if it is a first implementation of a tiered storage infrastructure. In this circumstance, enterprise management needs to carefully balance the costs (in real dollars and management distraction) with the ultimate risks of audit and punishment and operational and other savings that will accrue from the investment. For some organizations, compliance pressures can be a positive stimulus to IT systems process improvement.

Gartner's COMPARE, a Framework for Achieving Overall Compliance

The Gartner Group has developed a useful and unique methodology to ease compliance. COMpliance Progress And REadiness (COMPARE) is a well-defined framework for compliance projects with step-by-step processes that help compliance teams meet and then track compliance requirements. With COMPARE, organizations and businesses will be better prepared to respond to new and evolving compliance requirements.

Step 2. Understand the Products and Solutions Available to Support Your Compliance Efforts

Application Optimized Storage solutions for compliance are designed to help organizations minimize the time and cost of achieving compliance with Sarbanes-Oxley, HIPAA, and other regulations. A list of appropriate solutions to choose from is shown in Table 4, followed by a discussion of selected Hitachi compliance products and solutions. See the Hitachi Solutions Guide⁵ for a more detailed discussion of all Hitachi Data Systems solutions.

⁵ This guide is available from your Hitachi Data Systems sales representative.

Table 4. Application Optimized Storage Solutions that Support Compliance with Industry Regulations

| Storage Regulations | Storage Requirements | Hitachi Data Systems Solutions* | |
|---|---|---|---|
| | | Infrastructure Simplification Solutions | Business Continuity and Disaster Recovery Solutions |
| SOX Sections 301, 302, 802(a), 802(a)(1), 802(a)(2) Regulations S-X, Rule 2-06 | Require all audit and review information to be retained for 7 years | Consolidation, aggregation, tiering with DLM, and secure archiving for audit data | Open backup and recovery, mainframe backup and recovery, and disaster prevention planning and recovery solutions are recommended or required for all regulated data, depending on the language of specific laws and regulations |
| HIPAA Sec 1173(d)(2) | Requires medical records data to be maintained for 6 years, or 2 years after a patient's death | Consolidation, aggregation, and tiering with DLM and secure archiving for patient data | |
| FDA Rule 21 CFR Part 11 | Requires common portable formats for electronic information and signatures to preserve original content and meaning for 2 years (food), 3 years (drugs), or 5 years (biologics) for manufacturing processing, and packing | Consolidation, aggregation, and tiering with DLM and secure archiving for records on product development, clinical testing, manufacturing, and distribution | |
| GLBA (Gramm-Leach-Bliley) "Safeguards Rule" 16 CFR Part 314 | Requires technical structures to protect privacy and integrity of personal consumer information | Consolidation, aggregation, and tiering with DLM and secure archiving for all regulated consumer data | |
| SEC Rule 17a-3 and 17 a-4 | Requires firms to "make" records (17a-3) Requires storing and retrieval of records on WORM storage (17a-4) | Consolidation, aggregation, and tiering with DLM, including the Message Archive for E-mail solution and the Message Archive for Compliance solution, with partitioning for regulated trading data | |
| SEC Rule 17ad-6 and 17ad-7 | Requires storage mechanisms for ensuring accessibility, security, and integrity of records (17ad-6) Requires "means to recover data" (17ad-7) | | |
| NASD 3010 and 3110 | Requires supervision of client communications, including e-mail messages (NASD 3010) Requires retention of correspondence and data to meet SEC Rule 17a-4 (NASD 3011) | | |
| NYSE Rule 440 | Requires broker-dealers to make and preserve records per SEC Rule 17a-3 and 17a-4 | | |

* See also Appendixes C and D for specific hardware, software, and services for implementing a particular Application Optimized Storage solution.

Table 4. Application Optimized Storage Solutions that Support Compliance with Industry Regulations (Continued)

| Storage Regulations | Storage Requirements | Hitachi Data Systems Solutions | |
|---|--|--|---|
| | | Infrastructure Simplification Solutions | Business Continuity and Disaster Recovery Solutions |
| CFTC Rule 17 CFR Part 1 amendment to CFTC Regulation 1.31 | Requires a reliable records system to store electronic data for 5 years | Consolidation, aggregation, and tiering with DLM and partitioning for all regulated data requiring ILM management, depending on the interpretation of the legislation or law | Open backup and recovery, mainframe backup and recovery, and disaster prevention planning and recovery solutions are recommended or required for all regulated data, depending on the language of specific laws and regulations |
| NARA Part 1234 | Requires reliable records systems for all federal agencies, including access, retrieval, indexing, portability, backup and recovery, and archiving | | |
| DoD 5015.2 | Requires records management based on NARA, including safeguards against disaster | | |
| FISMA, COOP and COG, FOIA, NIST 800-34 and 800-53 | Require sound data security, backup and recovery, business continuity planning, and disaster recovery for government agencies and contractors | | |
| GASB Statement 34, June 1999 | Requires business continuity planning for all agencies operating a utility, so that their mission can continue in time of crisis or disaster | Recommended | All solutions are required |
| NERC Rule 1200 (1216.1) | Requires mandatory disaster recovery plans by the end of 2005 for electricity companies | Recommended | All solutions were required by year end 2005 |
| FERC Rules RM01-12-00 (Appendix G) | Set retention periods for public utilities and require protection from disaster | Recommended | All solutions are highly recommended |

Hitachi Archiving Products

Message Archive for Compliance Solution Preserves Messages for Mandatory Retention Periods

Part of the Infrastructure Simplification Solutions, the Message Archive for Compliance solution was developed to help you optimize your e-mail system while providing message indexing, search and retrieval capabilities, audit trails, and policy management to preserve messages for mandatory retention periods. As shown in Figure 2, Message Archive for Compliance enables you to retain an unalterable archive of e-mail and instant messages for the fixed period of time mandated by SEC Rule 17a-4, Sarbanes-Oxley, Basel II, and other regulatory requirements. WORM optical and tape media have traditionally been used for compliance with these regulatory requirements, because of their nonerasable and non-rewritable storage capabilities. Although optical and tape media continue to be used, they are not ideal, because the SEC, for example, requires that electronic records be easily accessible for a period of two years and SOX for a period of five years—making it difficult to use tape media.

Data Retention Utility Provides Disk-based Tamperproof WORM Capabilities

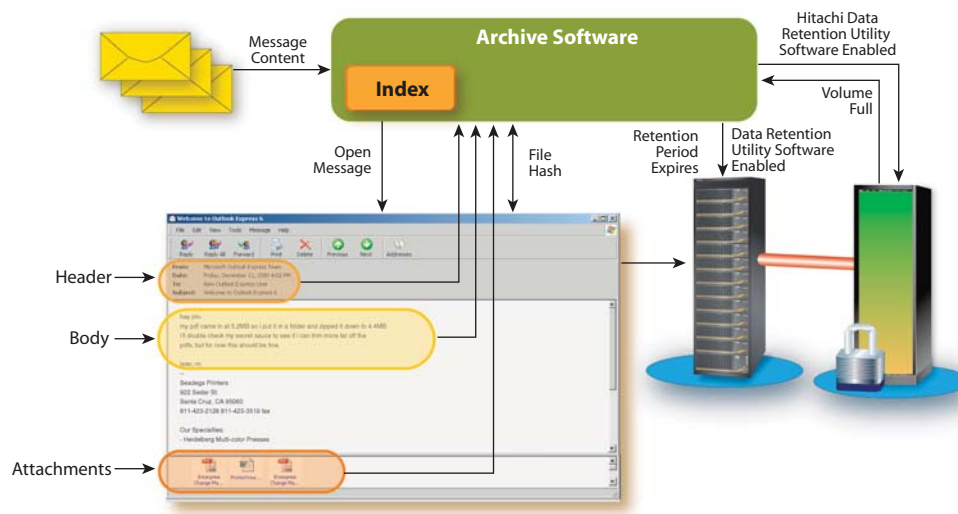
To solve these tape-media-related problems, storage vendors have developed a new breed of storage combining new cost-effective storage systems with WORM safeguards to deliver what some analysts

have dubbed a “WORM disk” storage solution that is ideal for regulated data storage compliance. The Data Retention Utility provides functionality on ATA-based storage systems to create large, economical storage systems that can deliver terabytes of online capacity at a TCO that is often less than or equivalent to that of tape when the people-intensive labor costs of operation are tallied. The Data Retention Utility’s tamperproof WORM software is available now on Universal Storage Platform systems, Lightning 9900 V Series systems, and Adaptable Modular Storage or Workgroup Modular Storage systems with SATA drives.

Example: A consulting company has decided to implement e-mail retention policies for regulatory and legal purposes as well as good business practice, but the company doesn’t want to purchase and manage dedicated WORM storage.

Solution: The company uses the NSC55 storage system already storing its Exchange databases. It implements the Message Archive for Compliance solution (see Figure 2) and the Data Retention Utility to turn its existing disk storage into a WORM device for message retention. Implementation is quick, retention is automated according to policies, and the ongoing cost of managing the solution is minimal.

Figure 2. Message Archive for Compliance Solution



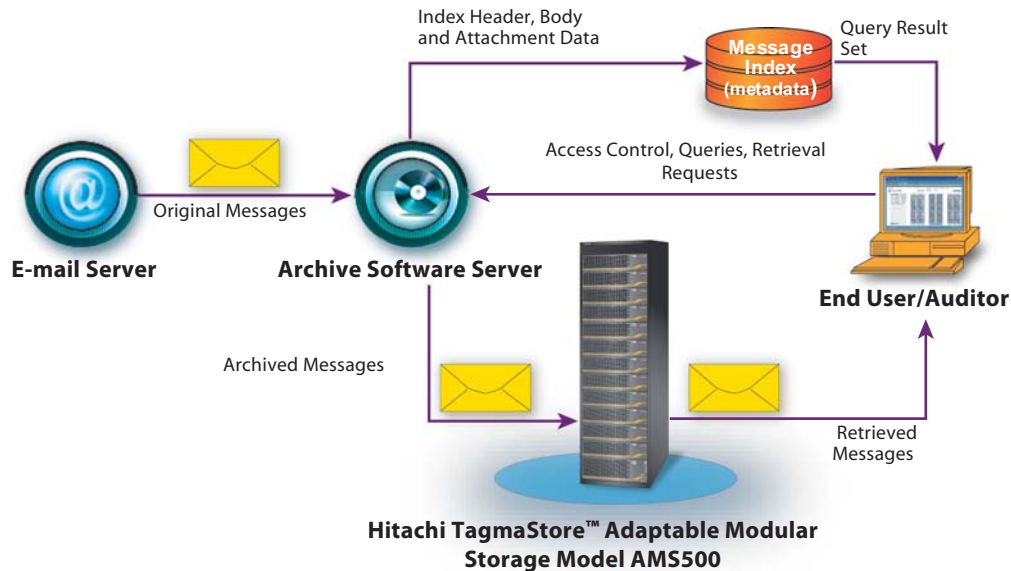
Message Archive for Compliance enables companies to retain an unalterable archive of e-mail and instant messages for the fixed period of time required by Sarbanes-Oxley and other regulations.

Message Archive for E-mail Solution

The Message Archive for E-mail solution leverages the standard Hitachi archival platform to provide automatic and selective document archiving, along with search-and-retrieval capabilities and audit trails. Figure 3 illustrates how e-mail archiving works in the data lifecycle. When data is introduced to the archive, a digital signature is assigned to uniquely identify the object and make sure it has not been tampered with. The object is then indexed, and metadata is created to describe the object in the message archive’s metadata store. Metadata is information about the data that is used in populating, maintaining, and accessing both the descriptive information that identifies the archive’s holdings and the administrative data used to manage the archive. In the Message Archive for E-mail solution, the only metadata needed might be the sender, date and time sent, subject line, and information about any

attachments (filename, size). In addition to providing users with a view of archived information, the solution seamlessly integrates into the client interface for Microsoft Outlook and Lotus Notes. Importantly, it eliminates “mailbox limit exceeded” problems, effectively expanding overall storage capacity for your e-mail users.

Figure 3. Message Archive for E-mail Solution



With the Message Archive for E-mail solution, the enterprise gains compliance and the user gains an unlimited mailbox.

Hitachi Data Protection Suite Unifies Data Backup and Recovery, Migration, Archiving, and Replication

The Hitachi Data Protection Suite, powered by CommVault®, is a unified platform comprising solutions for data backup and recovery, migration, archiving, and replication—all through a single easy-to-use point of control. Using the CommVault Common Technology Engine (CTE) as its foundation, the Data Protection Suite enables organizations to select the combination of products that best meets their needs.

Designed for disk-to-disk storage area network (SAN)-based data protection, the Data Protection Suite avoids the performance issues of products that have evolved from local area network (LAN)-based disk-to-tape infrastructures. Its CTE foundation enables the Data Protection Suite to help organizations implement the right mix of components without adding complexity. The Data Protection Suite includes the following software components:

- :: Hitachi Data Migrator
- :: Hitachi Quick Recovery
- :: Hitachi Data Archiver
- :: Hitachi Data Protection Monitor
- :: Hitachi Backup and Recovery

Hitachi HiCommand® Protection Manager Software

Most businesses rely heavily on e-mail and various database applications, not only for daily operations but also for compliance with government regulations. For most organizations, an outage in either environment essentially shuts down operations. The cost of any outage is steep, and repeated outages are not acceptable. The Hitachi HiCommand Protection Manager software is a disk-to-disk-based, rapid backup and recovery software program for Microsoft Exchange Server and Microsoft SQL Server environments that integrates and automates disk-to-disk backup and rapid recovery, using proven Hitachi replication technologies. Protection Manager software shrinks backup windows and improves the recovery time objective of Microsoft Exchange Server and SQL Server.

Protection Manager software supports Hitachi storage, including the Universal Storage Platform, Network Storage Controller, Adaptable Modular Storage model AMS500, and Hitachi Thunder 9585V™ ultra high-end modular storage. Protection Manager software is used in conjunction with Hitachi business continuity software products, specifically one or more of the following:

- :: **Hitachi ShadowImage™ In-System Replication software.** The high-speed, nondisruptive technology of ShadowImage software rapidly creates multiple copies of mission-critical information within Hitachi storage systems. At the same time, it keeps data RAID-protected and fully recoverable—without affecting service or performance levels. ShadowImage software copies can provide immediate nondisruptive access and sharing of information for decision support, testing and development, or optimization of tape backup operations.
- :: **Hitachi TrueCopy™ Remote Replication Software.** TrueCopy software provides a continuous, nondisruptive, host-independent remote-data-replication solution for disaster recovery or data migration over any distance. For locations within the same metropolitan area, TrueCopy software's synchronous mode provides a no-data-loss, rapid-restart solution, and its asynchronous mode ensures data consistency and rapid recovery over any distance.
- :: **Hitachi Universal Replicator Software.** Universal Replicator software delivers simplified remote asynchronous data replication for the Universal Storage Platform and the Network Storage Controller. Universal Replicator software's significant advantage over competitive products derives from advanced technology that offers lower overhead and improved link- or system-failure recovery and resynchronization performance.
- :: **Hitachi Copy-on-Write Snapshot Software.** Copy-on-Write Snapshot software is an alternative to ShadowImage software that provides logical snapshot data replication within Hitachi storage systems for immediate use in decision support, software testing and development, data backup, or rapid-recovery operations. Because only changed data blocks are stored, the amount of storage capacity required for each snapshot copy is substantially smaller than the source volume.

Services from Hitachi Data Systems Help Achieve Regulatory Compliance

Storage Economics Strategy Service Offers a Practical Way to Build a Business Case

Perhaps the most practical way to conduct your investment analysis of storage-related regulatory compliance investments is to engage Hitachi Data Systems Global Solution Services (GSS) consultants to work with you. The service that is offered to fill this need is the Storage Economics Strategy Service. Using the HiReturn tool, GSS experts will work with your storage and IT executives to determine the financial returns that a unified enterprisewide storage infrastructure can bring in mitigating regulatory compliance risks facing an enterprise.

Using best consulting practices, GSS consultants will help you simplify your storage infrastructure, fine-tune your DLM strategy, and help you implement an effective tiered storage infrastructure with policies for data that the enterprise deems important enough to be under regulatory control. Most importantly,

the Storage Economics Strategy Service helps you build a convincing business case for an investment in Hitachi storage solutions you select. A unique benefit of this service is that, unlike competitive solutions, it takes an approach that avoids the early retirement of existing storage assets before full depreciation. Not only is the HiReturn model competition-agnostic but the Storage Economics Strategy service is also competition-friendly. Competitors are not disparaged. Service results “tell it like it is” and let you decide.

The Storage Economics Strategy Service and HiReturn tool will graphically demonstrate to your executives the bottom-line impact of spending on any new storage hardware, software, or services you might acquire, plus the ongoing cost of storage ownership. Included are the following:

- :: Assessment of your enterprise storage infrastructure and needs
- :: Design of a new multitier, multivendor, centrally managed architecture in a collaborative workshop
- :: Analysis of ROI for multiple design options and multiple payback elements
- :: Justification and quantification of your storage direction in a custom, detailed report

Ultimately, a business case for an appropriate Hitachi Data Systems storage system or solution investment will cover the specific set of hardware, software, and services that creates a solid tiered storage infrastructure to facilitate regulatory compliance efforts.

Risk Analysis Workshop

The structured, interactive Risk Analysis Workshop from GSS provides a framework for quickly assessing your organization’s backup and recovery, business continuity planning, and disaster recovery environment at a high level. Working with your team, Hitachi Data Systems experts jointly score your organization’s current business continuity environment, identify areas of improvement, and objectively map them to potential solutions that can help your organization realize a higher degree of business continuity. Consultants then jointly formulate a diagnostic review that identifies specific strengths and limitations. The materials this service produces will assist your team in both understanding and articulating these findings and recommendations and how your backup and recovery and business continuity/disaster recovery policies and procedures can support your regulatory compliance efforts.

Business Continuity Strategic Technology Planning Service

As you prepare to plan and define your approach to business continuity and regulatory compliance, Hitachi Data Systems can provide a tiered storage architecture to support your business continuity/disaster recovery strategy. Hitachi Data Systems consultants assess your DLM and business recovery objectives and create a technology plan that defines your IT disaster recovery infrastructure. This plan specifies the appropriate technology, software, and resources you will need in order to create a strategy and an infrastructure capable of mitigating and recovering from incidents and outages, therefore supporting your regulatory requirements. GSS provides a definition of your recovery strategy; a written technology plan; project resource identification; financial estimates; and a strategic technology plan to encompass not only regulatory compliance objectives but also best practices for corporate data governance for storage, processing, and telecommunications.

Product and Solution Implementation Services

For all Hitachi products and solutions, GSS provides services to assist you in implementing compliance plans and procedures. The Message Archive for E-mail solution and Message Archive for Compliance solution require hardware, software, and implementation services. In addition, a full portfolio of product-based services is available for all Hitachi products and solutions necessary to implement an Application Optimized Storage solutions environment.

Step 3. “Short-list” Available Solutions and Services for Implementation

The process of short-listing vendor products to meet your regulatory compliance requirements can be time-consuming and require complex comparative analysis of many vendor tools. It is important to note that unlike other vendors, Hitachi carefully tests each product and solution for compatibility with other Hitachi and third-party products before general release. The products highlighted in Step 2 above are part of solutions involving both required and recommended hardware, software, and services for effective, error-free implementation. To simplify the process of designing and implementing Hitachi solutions, however, Hitachi Data Systems sales personnel and expert consultants can help guide you in architecting an effective tiered storage infrastructure as a basis for sound implementation of Application Optimized Storage solutions. You can choose to implement either single products or complete solutions such as infrastructure simplification or business continuity/disaster recovery. Appendix C and Appendix D contain descriptions and summaries of the benefits of these solutions to provide a planning perspective. These appendices define the key elements of Application Optimized Storage solutions and list both required and recommended hardware, software, and services for each solution.

Step 4. Determine ROI

In determining the value of Hitachi products and compliance solutions, you need to look at the “total business value,” which includes both hard and soft CapEx and OpEx cost savings and the value of improvements to the business from using the product or solution. These calculations must take into account the staggering projected growth of backup volume and requirements and the ongoing Moore’s Law–type drop in the price of physical storage, particularly disk storage. Although the focus may be on compliance for a particular project, it is wise to conduct a thorough analysis of the value of an investment in Hitachi storage solutions for presentation to your organization’s economic decision makers such as the CFO, CIO, and CEO. It can show them the return on the total investment from not only regulatory compliance but also from all other perspectives of corporate data governance. The HiReturn tool can help you weigh the cost/benefit trade-offs of an investment in Hitachi Data Systems solutions as compared to your current infrastructure. It can also compare Hitachi investment alternatives with those of competitors, because it is vendor-agnostic. The program can evaluate investments by using either the popular TCO or the discounted internal ROI methods.

The first step is to evaluate which use-case models (such as disaster risk or scheduled downtime) available in the HiReturn program should be run for your particular solution justifications. The Hitachi Data Systems sales team and consultants can help you apply this tool yourselves, or GSS can be engaged to complete the investment analysis for you.

Step 5. Implement Auditing and Monitoring

After you have received approval to implement a particular regulatory compliance investment, Hitachi Data Systems can provide a full set of services to assist you in technical project implementation of and training for the plan you created in Step 3. (See Appendix C and D for specific implementation details.) Once the compliance plan is implemented, it is important to include all procedures for records retention, backup and recovery, and business continuity/disaster recovery. Compliance plan auditing and monitoring are particularly important, because such plans not only provide for smooth operations but also serve as preventive measures that can provide legal protection when the procedures are followed, as was the case in the aforementioned Arthur Andersen Supreme Court case.

The Benefits of Using Application Optimized Storage Solutions for Compliance

Customer Case Study

This case study looks at one data center doing an infrastructure refresh as a part of a compliance project. The benefits of both business continuity/disaster recovery and infrastructure simplification solutions were considered. The customer “before” and “after” data center storage inventory is listed in Table 5.

Table 5. “Before” and “After” Storage Infrastructure in a Customer Case Study

| Category | Current Status | Application Optimized Storage™ Solution |
|-------------------|---|---|
| Storage inventory | <ul style="list-style-type: none"> 5 older EMC Symmetrix frames with 8TB usable capacity each 3 DMX1000s with 5TB each 6 Hitachi Thunder 9500™ V Series modular storage systems with point-to-point and SAN connection and an average of 6TB each 4 NetApp FAS960s with 10TB each 1 Centera for ECA with 20TB Total usable capacity = 121TB | <ul style="list-style-type: none"> Move the capacity from the older Symmetrix systems to a Universal Storage Platform (30TB total) Move the Thunder 9500 V Series systems behind the Hitachi TagmaStore™ Universal Storage Platform Move the ECA/NAS solutions behind the Universal Storage Platform. |
| SAN inventory | <ul style="list-style-type: none"> 3 medium Fibre Channel switch fabrics 1 IBM ESCON® director 4 NAS environments | <ul style="list-style-type: none"> Directors for Fibre Channel SAN and IBM® FICON® NAS filers replaced with Hitachi NAS Blade for TagmaStore Universal Storage Platform and Network Storage Controller Directors can be used in the back end Fibre Channel switches replaced with Fibre Channel directors |
| Hosts | <ul style="list-style-type: none"> 2 of the Symmetrix frames connected to IBM® S/390® servers 50 UNIX servers on 2 SANs 240 Microsoft Windows NT servers on NAS and SAN Several hundred more DAS WinTel hosts | <ul style="list-style-type: none"> Universal Storage Platform connects with FICON to mainframe, Fibre Channel directors to UNIX, and Windows NT to NAS Blades Host domain partitioning is used to segment workloads |

Table 5. “Before” and “After” Storage Infrastructure in a Customer Case Study (Continued)

| Category | Current Status | Application Optimized Storage™ Solution |
|---------------------------------|---|---|
| Second-site disaster recovery | 2 Symmetrix frames 1 Thunder 9500 V Series system 1 DMX 20 miles away No disaster recovery capabilities for half of the infrastructure | 1 Universal Storage Platform for universal replication enables disaster recovery protection capability for all hosts and data A 30 percent reduction of second-site storage is due to consolidated replication |
| Management operations and tools | EMC for Symmetrix EMC for Centera NetApp tools HiCommand software for Thunder 9500 V Series systems | Hitachi HiCommand® software and other Universal Storage Platform software are required This is where quality of service via a virtual port comes in |
| Labor | Separate teams for mainframe, UNIX, and Windows NT EMC team (8 FTE) Hitachi Data Systems storage team (3 FTE) NetApp team (1 FTE) SAN team (2 FTE) Unknown FTE for Windows DAS | Unified storage and SAN team with Universal Storage Platform 2 FTE for all storage 2 FTE for backup and disaster recovery 2 FTE for SAN |
| Risks | Outage with NAS not uncommon Disaster recovery failover that does not always work Several hours per year for .bin file changes Microcode on the SANs | High-availability configurations and virtual storage segmentation isolate key applications from less tolerant ones Effective scheduled outage: 1 per year; 99.999% target for main storage operations |
| Utilization | S/390 ~ 70% Windows NT on SAN ~ 30% UNIX ~ 45% Windows NT on NAS ~ 40% Windows NT DAS ~ 20% | Aggregate tiered utilization rate of 75% |

Economic Benefit Summary

From a financial point of view, the HiReturn ROI tool from Hitachi Data Systems projected the economic parameters shown in Table 6:

- :: Investment of US\$3.9 million
- :: Total savings of US\$15.8 million over four years
- :: Internal rate of return (IRR) of 9.5 percent
- :: Payback in 16 months
- :: Discounted internal rate of return on investment of nearly 300 percent

Table 6. HiReturn Financial Results over Four Years

| | Year 1 | Year 2 | Year 3 | Year 4 | |
|---|--|--|-------------|--------------|------------------------|
| Cash investment in (US dollars) | (\$4,585,000) | \$180,000 | \$187,688 | \$240,375 | |
| Savings | | | | | Use-case totals |
| Administrative savings | 0 | 614,056 | 1,607,410 | 3,217,425 | 5,438,891 |
| Availability savings | 197,100 | 197,100 | 197,100 | 197,100 | 788,400 |
| Disaster risk savings | 250,000 | 250,000 | 250,000 | 250,000 | 1,000,000 |
| Avoidance of fines and sanctions | Hitachi Data Systems recommends that this analysis be presented without quantification of these savings, because the TCO/ROI is usually an adequate justification of the investment. | | | | |
| Environmental savings | 15,814 | 24,466 | 38,042 | 59,468 | 137,790 |
| IBM® FICON® versus IBM ESCON® savings | 88,626 | 88,626 | 88,626 | 88,626 | 354,504 |
| Hardware maintenance | 170,000 | 209,750 | 550,429 | 808,494 | 1,738,673 |
| Management and automation savings | 76,140 | 77,663 | 79,216 | 80,800 | 313,819 |
| Scheduled downtime | 71,692 | 71,805 | 71,922 | 72,040 | 287,459 |
| Software maintenance | 230,000 | 80,000 | 70,000 | 70,000 | 450,000 |
| Utilization improvement | 2,481,189 | 831,126 | 948,927 | 1,094,493 | 5,355,736 |
| Net cash flow | (\$1,004,439) | \$2,624,593 | \$4,089,359 | \$6,178,821 | |
| Cumulative cash flow | (\$1,004,439) | \$1,620,154 | \$5,709,513 | \$11,888,334 | |
| Total investment | \$3,976,938 | | | | |
| Total savings | \$15,865,271 | | | | |
| Client-supplied internal rate of return | 10.00% | | | | |
| Calculated internal rate of return | 9.49% | | | | |
| Net present value (NPV) of savings | \$5,196,835 | | | | |
| ROI using the "benefit over investment" method | 299% | [Savings – investment]/ investment | | | |
| ROI using the "net present value" method | 140% | NPV of savings / net present value of investment | | | |

As shown also in Table 5, and as is typical with most storage infrastructure investments, both regulatory compliance and non-compliance-related benefits occurred. This customer case projected the following compliance-related benefits in DLM, backup and recovery, and business continuity/disaster recovery:

- :: Scheduled downtime was decreased.
- :: Availability was increased, with reduced business impact and SLA penalties and higher customer satisfaction.
- :: Disaster risk was reduced.
- :: Data replication function was simplified, less software used, and less staff time required.
- :: Circuit costs of the disaster recovery site were reduced through simplification.
- :: Eight fewer people were needed to manage the storage infrastructure and disaster recovery site.
- :: The life of the enterprise content archival storage was extended.

Many non-compliance-related benefits were also realized in the areas of simplification, consolidation, aggregation, tiering, and DLM:

- :: Aggregate utilization improvements reduced the total data store by 11TB, to avoid unnecessary purchases.
- :: Aggregate utilization improvements will reduce the total data store by 180TB in the next four years.
- :: Seven frames were removed, with the associated benefits of hardware, software maintenance, floor space, and electricity reduction.
- :: The older Fibre Channel switch and IBM ESCON® director were removed, for more hardware maintenance savings.
- :: Storage management software license fees were reduced.
- :: SAN complexity was reduced, for easier management.
- :: Hardware maintenance for older Symmetrix systems was eliminated.
- :: Service-level agreement and tiered storage were made available for all storage customers (the mainframe can use a SATA disk for enterprise content archiving).
- :: The footprint was reduced; electricity and A/C costs stay about the same.

ROI conclusions

The Application Optimized Storage solutions and Universal Storage Platform models proposed in this customer example show many technical benefits in simplifying storage management, reducing storage labor, and minimizing data migration and replication while achieving regulatory compliance benefits. Further benefits and savings come from having fewer frames as a result of the consolidation. In this example, many older enterprise content archival systems were kept and the investment from the customer stayed intact. This example shows that the Application Optimized Storage solutions, combined with a Universal Storage Platform investment, can provide a single management framework that reduces cost by eliminating redundant management applications and using fewer personnel to manage a complex environment, versus a simpler system. The ROI results are conservative and believable, because not all savings come from one area. Rather, there is a blended rate of savings in labor, environmental costs, maintenance fees, utilization improvements, future purchase avoidance, and risk. Labor, risk, and utilization tend to be the largest cost drivers that can be limited with these types of activities, and this model confirms this to be true.

As in this case study, the key in developing economic models for regulatory compliance is to look for and quantify a variety of projected benefits. Hitachi solutions are so broad and strong that new savings are constantly uncovered throughout the process. This case study has demonstrated the huge economic benefits of an Application Optimized Storage tiered architecture combined with a Universal Storage Platform and remapping of existing storage equipment. The customer was able to address the key business initiatives of regulatory compliance, business continuity, simplified storage area management, and effective DLM with Hitachi products better than with any other offering. A key to success is the ability to translate the requirements of compliance into an overall improved storage infrastructure, with a broad range of other business values.

Reduced Cost and Time to Achieve Compliance

Because compliance involves establishing the ability to adhere to various regulations and, in the case of SOX, most executives require internal compliance audits to prepare for the possibility of an actual audit, you want to be in a position to quickly and cost-effectively provide necessary messages, data, and information for these internal “dry runs,” with minimum disruptions to IT operations and personnel. Hitachi Data Systems automated and cost-effective Application Optimized Storage framework and tiered infrastructure are ideal solutions, therefore, for both internal and external compliance audits. The process of seeking approval for proposed compliance investments will also put the IT storage group in a favorable light, by taking the big-picture approach described in this paper.

Benefits of Infrastructure Simplification Solutions

Infrastructure Simplification solutions from Hitachi Data Systems reduce CapEx and OpEx not only through consolidation aggregation but also through tiered storage, DLM, and partitioning storage solutions. Tightly integrated through common management and storage virtualization software, Application Optimized Storage solutions fully leverage your current storage investments while better aligning them for future growth. Centralized uniform storage management methodologies are probably the only cost-effective and timely way to prepare for a compliance audit for today's 24/7 worldwide enterprise.

Benefits of the Business Continuity/Disaster Recovery Solutions

Many regulations are not specific but set goals for business continuity and the ability to restore operations and services quickly in the event of a disaster such as a hurricane, earthquake, tsunami, or terrorist attack. Business Continuity and Disaster Recovery solutions from Hitachi Data Systems include enhanced backup and recovery solutions for both open systems and mainframe environments that the competition just can't match. Known for decades as the industry leader in high-availability data storage products, Hitachi Data Systems now provides business continuity/disaster recovery and backup and recovery solutions that offer unsurpassed consulting services and technical excellence in disaster prevention and planning, as well as recovery solutions that are the industry's most advanced and will result in both hard and soft CapEx and OpEx savings for the enterprise.

Appendix A: Acronyms

| | | |
|---------|---|---|
| BIA | — | business impact analysis |
| CapEx | — | Capital Expense |
| CFR | — | Code of Federal Regulations |
| CFTC | — | Commodity Futures Trading Commission |
| CIPC | — | Critical Infrastructure Protection Committee |
| COBIT | — | Control Objectives for Information and related Technology |
| COG | — | continuity of government |
| COOP | — | continuity of operations |
| COMPARE | — | COMpliance Progress And REadiness |
| COSO | — | Committee of Sponsoring Organizations |
| CTE | — | common technology engine |
| DLM | — | data lifecycle management |
| DoD | — | Department of Defense |
| EFA | — | expedited funds availability |
| ERM | — | electronic records management |
| FCC | — | Federal Communications Commission |
| FDA | — | Food and Drug Administration |
| FDIC | — | Federal Deposit Insurance Corporation |
| FERC | — | Federal Energy Regulatory Commission |
| FFIEC | — | Federal Financial Institutions Examination Council |
| FISMA | — | Federal Information Security Act |
| FOIA | — | Freedom of Information Act |
| FRB | — | Federal Reserve Bank |
| FRS | — | Federal Reserve System |
| GASB | — | Governmental Accounting Standards Board |
| GLBA | — | Gramm-Leach-Bliley Act |
| HIPAA | — | Health Insurance Portability and Accountability Act |
| ILM | — | information lifecycle management |

| | | |
|-------|---|--|
| ISO | — | International Organization for Standardization |
| ITL | — | Information Technology Laboratory |
| NARA | — | National Archives and Records Administration |
| NASD | — | National Association of Securities Dealers |
| NCUA | — | National Credit Union Administration |
| NERC | — | North American Electric Reliability Council |
| NIST | — | National Institute of Standards and Technology |
| NYSE | — | New York Stock Exchange |
| OCC | — | Office of the Comptroller of the Currency |
| OTS | — | Office of Thrift Supervision |
| PCAOB | — | Public Company Accounting Oversight Board |
| PHI | — | protected health information |
| ROI | — | return on investment |
| SEC | — | Securities and Exchange Commission |
| SOX | — | Sarbanes-Oxley Act |
| SMS | — | systems managed storage |
| SP | — | special publication |
| SRM | — | storage resource management |
| TCO | — | total cost of ownership |
| WORM | — | write once, read many |

Appendix B: Storage Regulations Affect All Industries

Sarbanes-Oxley

The Sarbanes-Oxley (SOX) Act of Congress, 2002, is a corporate financial reform bill intended to restore investor confidence in U.S. public markets that was eroded after the collapse of Enron and MCI. SOX is intended to make public reporting of corporate financials more accurate, transparent, timely, and accountable to shareholders of SEC-regulated companies. Although nothing in SOX requires the use of any particular technology or application, many auditors look to sound auditing and ERM applications and tiered storage infrastructures for solutions. The military specification DoD 5015.2 is considered by many IT professionals to be a sound set of rules to follow to meet the ERM requirements of SOX. (See the DoD 5015.2 section below.)

Section 301 of the Sarbanes-Oxley Act requires all organizations governed by the SEC to establish and maintain an audit committee that must appoint a registered public accounting firm to report to that committee. Section 302 of the Act requires that corporate officers certify periodic financial reports and that the reports contain accurate information that is not misleading. Criminal penalties and fines are prescribed for violations of these requirements.

Section 802(a) of the Sarbanes-Oxley Act

Section 802(a) of the Sarbanes-Oxley Act imposes criminal penalties of fines and/or up to 20 years imprisonment for violations:

“Whoever knowingly alters, destroys, mutilates, conceals, covers up, falsifies, or makes a false entry in any record, document, or tangible object with the intent to impede, obstruct, or influence the investigation or proper administration of any matter within the jurisdiction of any department or agency of the United States or any case filed under title 11, or in relation to or contemplation of any such matter or case, shall be fined under this title.”

Section 802(a)(1) of the Sarbanes-Oxley Act

Section 802(a)(1) of SOX defines the period for records storage:

“Any accountant who conducts an audit of an issuer of securities to which section 10A(a) of the Securities Exchange Act of 1934 (15 U.S.C 78j-1(a)) applies, shall maintain all audit or review workpapers for a period of 5 years from the end of the fiscal period in which the audit or review was concluded.”

Section 802(a)(2) of the Sarbanes-Oxley Act

Section 802(a)(2) of SOX defines the type of records, data, and communications that need to be stored, including electronic records:

“The Securities and Exchange Commission shall promulgate, within 180 days, such rules and regulations, as are reasonably necessary, relating to the retention of relevant records such as workpapers, documents that form the basis of an audit or review, memoranda, correspondence, communications, other documents, and records (including electronic records) which are created, sent, or received in connection with an audit or review and contain conclusions, opinions, analyses, or financial data relating to such an audit or review.”

Although the exact method for storing this data is not specified, it is widely interpreted to be in a form unaltered from the original.

Although SOX is mainly about financial controls and because IT systems are used to generate, transport, and store financial data, IT systems need controls to ensure that an enterprise's financial reporting can stand up to SOX auditing. Because much marketing hype has surrounded SOX, Hitachi Data Systems wants to make it clear that Hitachi products and solutions are intended to provide a solid underlying storage infrastructure to support IT systems in achieving compliance. The Application Optimized Storage framework and solutions are presented as a common-sense approach to help meet the implicit enterprise storage requirements of SOX while improving overall data governance by the enterprise.

Storage Regulations Affecting the Health Care Industry

HIPAA "Security Rule" Section 1173(d)(2)

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, for six years, for 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. Specifically, Section 1173(d)(2) of the Act states:

"Each person described in section 1172(a) who maintains or transmits health information shall maintain reasonable and appropriate administrative, technical, and physical safeguards—(A) to ensure the integrity and confidentiality of the information; (B) to protect against any reasonably anticipated—(i) threats or hazards to the security or integrity of the information; and (ii) unauthorized uses or disclosures of the information; and (C) otherwise to ensure compliance with this part by the officers and employees of such person."

Many health care providers do not currently have radiology and other graphical data under the control of IT and should consider doing so unless the current system is trustworthy enough to meet HIPAA requirements. In many cases, this simply means applying backup and recovery and business continuity/disaster recovery systems and procedures as a networked back end to radiology departments' daily operations, for which local departments will be most likely be thankful when they have understood the benefits.

FDA Title 21 Code of Federal Regulations (21 CFR Part 11)

When firms regulated by the U.S. Food and Drug Administration (FDA) generate records in electronic form, their records storage systems are subject to rules specified in the Code of Federal Regulations (CFR), Chapter 21, Part 11, commonly known as 21 CFR 11 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 have used paper-based records to meet FDA

requirements, but they are increasingly keeping key records and documents in electronic form and storing them in computer-based applications and storage systems. Businesses within this definition need to reevaluate how data generated in research, clinical trials, regulatory approval, and manufacturing is maintained and preserved within the organization.

Storage Regulations Affecting the Financial Services Industry

The financial services industry in the United States consists of three main segments or types of business—securities, banking, and insurance—subject to specific sets of laws and regulations. Large financial holding companies may include business units operating in all three segments and across country borders. 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), and the like. Insurance firms are regulated primarily by state government agencies, although federal agencies are taking a closer look at insurance industry practices under laws such as the USA PATRIOT Act. Financial services firms are also subject to the Sarbanes-Oxley Act (U.S.) and the Data Protection Acts (EU). 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 and misleading financial reports. Regulatory agencies such as the SEC translate these legal mandates into rules and regulations.

Gramm-Leach-Bliley Act (GLBA) “Safeguards Rule” 16 CFR Part 314

All financial services firms are subject to the requirements of the Gramm-Leach-Bliley Act (GLBA), but there is no single enforcement agency for the 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 C). Signed by President Clinton in 1999, this act applies to all financial institutions as defined by the Federal Reserve and requires disclosure to customers of their policies and practices for protecting the privacy of nonpublic personal information. The act requires a technical structure to protect the privacy and integrity of personal consumer information and makes it a crime to fraudulently obtain personal information from a financial institution.

SEC Rule 17a-3

Rule 17a-3 lists the SEC requirements for “Records to Be Made by Certain Exchange Members, Brokers and Dealers.”

SEC Rule 17a-4

The SEC's "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 IT 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 WORM capability. Within the financial services sector, one securities firm category, the broker-dealer, is receiving particularly intense scrutiny from government regulators. 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. Among the best-known directives within SEC Rule 17 are the following:

- :: Written and enforceable retention policies
- :: Storage of data on indelible, nonrewritable media
- :: Searchable index of all stored data
- :: Readily retrievable and viewable data
- :: Storage of data offsite

In mid-2003 the SEC issued a clarification about what type of media constitutes valid storage media for the "indelible, non-rewritable media" language of Rule 17a-4 and accepted that certain disk/software combinations can qualify to meet this requirement. This means that Hitachi Data Retention Utility software, when combined with midrange ATA-based storage systems, is acceptable for data archiving purposes under this stringent rule. (See also "Data Retention Utility" in the section above titled "Application Optimized Storage Solutions Help the Enterprise Achieve Regulatory Compliance")

SEC Rule 17ad-6 and 17ad-7

These rules require storage mechanisms to ensure accessibility, security, and integrity of records in addition to a means for recovering data.

Basel II

Ratified in Basel, Switzerland, in 2004, the Basel II Accord⁶ has turned what used to be best practices into regulatory requirements for Financial Service Providers (FSPs) doing business in Europe as well as for companies operating in other parts of the world with headquarters in Europe. The accord deals with complex, risk-focused capital adequacy rules that affect 20 to 30 of the largest U.S. banks and require, for example, that banks put in place business continuity and disaster recovery plans to ensure operations in the event of a disaster and thereby limit losses.

NASD (National Association of Securities Dealers) Rule 3010 and 3011

These rules require supervision of all correspondence with customers, including outgoing e-mails and retention of correspondence and data to comply with SEC Rule 17a-4.

⁶ Basel II is also known as the "capital adequacy framework." The governors and supervisors met at the Bank for International Settlements in Basel, Switzerland, to review the text prepared by the Basel Committee on Banking Supervision.

NYSE (New York Stock Exchange) Rule 440

This rule requires broker-dealers to make and preserve records as per SEC Rules 17a-3 and 17a-4.

CFTC (U.S. Commodity Futures Trading Commission) 17 CFR Part 1 amendment to CFTC Regulation 1.31

This rule requires all commodity traders to maintain reliable records system to store electronic data for five years.

FFIEC

The Federal Financial Institutions Examination Council (FFIEC) Handbook, 2003–2004 (Chapter 10) covers business continuity planning requirements for a variety of financial institutions. It covers all companies regulated by the Federal Deposit Insurance Corp. (FDIC), Federal Reserve Bank (FRB), U.S. Office of the Comptroller of the Currency (OCC), Office of Thrift Supervision (OTS), Treasury Department, and National Credit Union Administration (NCUA).

Storage Regulations Affecting Government Agencies

FISMA

The Federal Information Security Act (FISMA) of 2002, Title III of the E-Government Act of 2002, is designed to keep government open and running during a crisis. Its emphasis is mostly on data security, and state and local governments can make their own decisions on data security, backup and recovery, and disaster recovery,, known in government parlance as “continuity of operations,” or COOP.

COOP and COG

Continuity of operations (COOP) and continuity of government (COG) refer to minimum planning requirements for federal government operations as delineated in the Federal Preparedness Circular 69, 26 July 1999. This directive states that a business continuity plan must be maintained at a high level of readiness and capable of being implemented without warning in a disaster or emergency and sustain itself for up to 30 days.

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 agencies are usually 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, but it is specified as a requirement.

NIST 800-34 and 800-53

The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-34, Contingency Planning Guide for Information Technology Systems, June 2002, requires contingency, disaster recovery, and COOP plans. NIST 800-53 is titled “Recommended Security Controls for Federal Information Systems, February 2005,” and lists mandatory security controls that became a federal standard at the end of 2005.

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:

- :: Method of retrieving desired documents
- :: Appropriate security to ensure integrity
- :: A standard interchange format, when necessary, to permit the exchange of documents on electronic media between agency computers⁷
- :: Disposition of the documents, including transfer of permanent records to NARA

NARA Part 1234.28 specifies records backup and recovery.

DoD 5015.2

Government and military record management application (RMA) product procurements are required to comply with DoD 5015.2. This specification requires an ERM system for creating, classifying, indexing, storing, retrieving, and copying of official records related to government procurements and is made available to vendors, developers and users⁸. NARA has endorsed this standard for use by all Federal agencies and is viewed by many as one that would meet the objectives of SOX in non-government and military applications. Here is a summary of its specifications:

1. Making records
 - :: Assign a unique record identifier to each record
 - :: Store a record and all attachments
 - :: Identify the media type, format, and location of all records
2. Classifying records
 - :: Provide the capability to organize all records
 - :: Provide the capability to assign a record classification code to each record
3. Indexing records
 - :: Uniformly create and maintain indexes for all records
4. Storing records
 - :: Maintain the integrity of records, and do not change the format of the record
5. Screening and disposing of records
 - :: Provide output for viewing, saving, and printing records
 - :: Notify authorized individuals of required disposition actions, based on both the category and the disposition instruction

⁷ This means both mainframe and open system servers and storage in the context of all NARA clients in government.

⁸ See also <http://jirc.fhu.disa.mil/recmgmt/standards.html>

6. Retrieving records
 - :: Provide the capability to request records by using the indexes
 - :: Present users a list of records meeting retrieval criteria
 - :: Provide record copies in the format in which they are stored
7. Copying records
 - :: Never allow modification of the stored record

Such a standard is fully met by Application Optimized Storage solutions implemented in conjunction with ERM applications and best records management practices. The ability of the Data Retention Utility to provide disk-based tamperproof WORM capability is implicit in the “copying of records” requirement of this specification.

Storage Regulations Affecting Public Utilities

GASB

The Governmental Accounting Standards Board (GASB) requires a business continuity plan for all agencies operating a utility, so that their mission can continue in a time of crisis or disaster.

NERC

North American Electric Reliability Council (NERC) 1200 (1216.1), 2003, made voluntary disaster recovery plans mandatory by the end of 2005. In addition, the NERC Security Guidelines for the Electricity Sector, June 2001, includes business continuity/disaster recovery information security standards for the industry/government partnership, as guided by the Critical Infrastructure Protection Committee (CIPC).

FERC

Federal Energy Regulatory Commission (FERC) RM01-12-00 (Appendix G), 2003, mandates recovery plans for all public utilities except rural utilities and limited distribution co-ops.

Appendix C: Description and Summary Benefits of the Infrastructure Simplification Solutions

Table 7. Description and Summary Benefits of Infrastructure Simplification Solutions

| Hitachi Infrastructure Simplification Solutions | | | | |
|---|---|--|---|--|
| | | Consolidation and Aggregation | Tiered Storage: Data Lifecycle Management | |
| | | | E-mail | Mainframe Application Data |
| Solution Elements | Definition | Consolidation of multiple workloads on a single Hitachi storage system Aggregation of external storage workloads for “single pane of glass” storage management | Message Archive for E-mail moves e-mail to modular storage with SATA Message Archive for Compliance retains data for mandatory periods | Match value of data to storage tier; replace tape with disk for faster access and quicker recovery |
| | Problem | Underutilized storage, SAN islands, multiple staffs and replication software; one storage tier does not fit all | Clogged e-mail servers Data cannot be kept in unaltered permanent form | Wasting enterprise disk for lower priority mainframe data, such as offline decision support applications or referential data |
| | Desired Result | Reduction of the number of storage management software platforms to be managed; better storage utilization; labor savings (OpEx) and delayed CapEx | Unclogs e-mail servers and eliminates “mailbox size limits” Retains unaltered data for specified period | Reduction of the high cost of enterprise storage and storage management by tailoring storage attributes to application priorities agreed with business managers |
| | Solution | All multivendor data managed by Hitachi HiCommand® Suite software Data virtualized into one or more logical pools on multiple tiers Existing storage frames retired or re-purposed to delay storage purchase cycle (CapEx) | Data lifecycle services automatically move or store data on modular storage with SATA drives at the required time and in the required format Reduced business risk | Place data for low-priority applications on Hitachi TagmaStore™ Adaptable Modular Storage or Workgroup Modular Storage systems with SATA drives or repurpose current storage to defer CapEx for new storage. |
| | Hardware | Hitachi TagmaStore™ Network Storage Controller (model NSC55) or Universal Storage Platform | Not required for consolidation One or more required for aggregation | One or more are required |
| Hardware | Hitachi TagmaStore™ Adaptable Modular Storage or Workgroup Modular Storage with SATA drives | Required for consolidation Optional for aggregation if Hitachi systems are being aggregated | Required for backup/archive | Required for backup/archive |
| | Existing Hitachi Lightning 9900™ V Series systems | Optional | Optional for second tier | Optional for second tier |
| | Existing Hitachi Thunder 9200™ and Thunder 9500™ V Series modular storage systems | Optional | Optional for second or third tier | Optional for second or third tier |
| | IBM, EMC, Sun, or HP systems | Optional | Optional | Optional |

Table 7. Description and Summary Benefits of Infrastructure Simplification Solutions (Continued)

| Hitachi Infrastructure Simplification Solutions | | | | |
|---|---|---|--|--|
| | | Consolidation and Aggregation | Tiered Storage: Data Lifecycle Management | |
| | | | E-mail | Mainframe Application Data |
| Required Software | Hitachi Universal Volume Manager | Required | Required | Required |
| | Hitachi HiCommand® Tiered Storage Manager | Recommended for consolidation Required if Hitachi systems are being aggregated | Required | Required |
| | Hitachi Data Retention Utility | Optional | Required for tamperproof archiving | Optional |
| | Basic Element Manager for Sun IBM or EMC | Required for each external storage system to be attached | Required for each external storage system to be attached | Required for each external storage system to be attached |
| | Hitachi HiCommand® Device Manager | Required | Required | Required |
| | Hitachi Resource Manager™ utility package | Required | Required | Required |
| | Hitachi HiCommand® Backup Services Manager, powered by APTARE® | N/A | N/A | Required |
| | Hitachi Resource Manager™ utility package for IBM® z/OS® | Required–mixed | N/A | Required |
| Basic Services | Message Archive for E-mail | N/A | Required to eliminate mailbox size limits | N/A |
| | Message Archive for Compliance | N/A | Required for tamperproof archiving | N/A |
| | External Storage Implementation Service for Hitachi TagmaStore™ Universal Storage Platform and Network Storage Controller | Basic/recommended | Basic/recommended | Basic/recommended |

Appendix D: Description and Summary Benefits of Business Continuity/Disaster Recovery Solutions

Table 8. Description and Summary Benefits of Business Continuity and Disaster Recovery Solutions

| Hitachi Business Continuity and Disaster Recovery Solutions | | | | |
|---|---|---|---|---|
| | Open Backup and Recovery | Mainframe Backup and Recovery | Disaster Prevention Planning and Recovery | |
| Solution Elements | Definition | Local or remote backup of disaster recovery volumes to Hitachi TagmaStore™ Adaptable Modular Storage or Workgroup Modular Storage SATA disk or tape | Offloading IBM® DFSMSHsm™ replication; saves IBM z/OS® cycles, frees storage, and reduces cost SATA disk backup; improves Tivoli z/OS backup-and-recovery efficiency, reduces TCO Replacing mainframe tape with “virtual tape” on SATA disk | Two-data-site “heterogeneous replication;” allows improved disaster recovery plan testing with current data “No data loss,” three-site, super-high-availability solution |
| | Problem | High cost of local backup to disk for fast restore | SMS is MIPS-intensive High disk cost keeps Tivoli disk storage pools small Long restore time from tape | Multiple-vendor disaster recovery software and storage resource management tools Lack of flexible disaster recovery for all storage systems |
| | Desired Result | Fast restores from local replication copies | Reclaim IBM® z/OS® MIPS Larger Tivoli disk storage pools Fast restore from tape volumes | One replication product for all storage systems, “single pane of glass” management, adequate testing of disaster prevention and disaster recovery plans |
| | Solution | Remote replication and point-in-time copies enable cost-effective backup to SATA disk locally or tape remotely | Storage-based replication SATA disk for disk backup Put virtual tape volumes on SATA disk | Improved disaster prevention and disaster recovery plan testing No-data-loss, three data center solution for the large enterprise |
| Hardware | Hitachi TagmaStore™ Network Storage Controller or Universal Storage Platform | One or more are required | One or more required for storage-based replication, SATA disk for disk backup, and putting virtual tape volumes on SATA disk | One or more are required |
| | Hitachi TagmaStore™ Adaptable Modular Storage or Workgroup Modular Storage with SATA drives | Optional | Optional | Optional |
| | Existing Hitachi Lightning 9900™ V Series systems | Optional | Optional for storage-based replication, SATA disk for disk backup, and putting virtual tape volumes on SATA disk | Optional |
| | Existing Thunder 9500™ V Series modular storage systems | Optional | Optional | Optional |
| | Hitachi TagmaStore™ Workgroup Modular Storage with SATA drives or Hitachi Thunder 9520V™ workgroup modular storage system | Required for backup | One or more required for storage-based replication, SATA disk for disk backup, and putting virtual tape volumes on SATA disk | One or more are required |
| | IBM, EMC, Sun or HP systems | Optional | Optional | Optional |

Table 8. Description and Summary Benefits of Business Continuity and Disaster Recovery Solutions (Continued)

| Hitachi Business Continuity and Disaster Recovery Solutions | | | | |
|---|---|--|---|--|
| | Open Backup and Recovery | Mainframe Backup and Recovery | Disaster Prevention Planning and Recovery | |
| Required Software | Hitachi Universal Volume Manager | Required | Required for storage-based replication, SATA disk for disk backup, and putting virtual tape volumes on SATA disk | Required |
| | Hitachi ShadowImage™ In-System Replication | Required | Required for storage-based replication Optional: SATA disk for disk backup and putting virtual tape volumes on SATA disk | Required |
| | Hitachi Compatible Mirroring software for IBM® FlashCopy® | Optional | Required | Optional |
| | Hitachi Dataset Replication software for IBM® z/OS® | Optional | Required | Optional |
| | IBM Tivoli Manager | Optional | Required | Optional |
| | Hitachi Universal Volume Manager | Required | Required for storage-based replication, SATA disk for disk backup, and putting virtual tape volumes on SATA disk | Required |
| | Hitachi ShadowImage™ In-System Replication | Required | Required for storage-based replication Optional: SATA disk for disk backup and putting virtual tape volumes on SATA disk | Required |
| | Hitachi Compatible Mirroring software for IBM® FlashCopy® | Optional | Required | Optional |
| | Hitachi Dataset Replication software for IBM® z/OS® | Optional | Required | Optional |
| | IBM Tivoli Manager | Optional | Required | Optional |
| | Hitachi HiCommand® Tiered Storage Manager | Optional | Required | Optional |
| | Basic Element Manager for Sun, IBM, or EMC | Required for each external storage system to be attached | Required for each external storage system to be attached | Required for each external storage system to be attached |
| | Hitachi HiCommand® Device Manager | Required | Required | Required |
| | Hitachi Resource Manager™ utility package | Required | Required | Required |
| | Hitachi HiCommand® Backup Services Manager software, powered by APTARE® | Required | Recommended | Required |
| | Hitachi Resource Manager™ utility package for IBM z/OS | Required–mixed | Required | Required |

Table 8. Description and Summary Benefits of Business Continuity and Disaster Recovery Solutions (Continued)

| Hitachi Business Continuity and Disaster Recovery Solutions | | | | |
|---|---|--------------------------|-------------------------------|---|
| | | Open Backup and Recovery | Mainframe Backup and Recovery | Disaster Prevention Planning and Recovery |
| Required and Basic Services | External Storage Implementation Service for Hitachi TagmaStore™ Universal Storage Platform and Network Storage Controller | Basic/recommended | Basic/recommended | Basic/recommended |
| | Implementation Service for Hitachi Data Protection Suite, powered by CommVault® | Required | Optional | Optional |

 **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. HiCommand is a registered trademark of Hitachi, Ltd.

Hi-Track is a registered trademark and Application Optimized Storage, Thunder 9500, Lightning 9900, TagmaStore, Thunder 9520V, Thunder 9570V, Thunder 9585V, TrueCopy, ShadowImage, HiReturn, are trademarks of Hitachi Data Systems Corporation.

CommVault is a registered trademark of CommVault Systems, Inc.

All other product and 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 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.

©2006, Hitachi Data Systems Corporation. All Rights Reserved.

WHP-210-00 January 2006