

# Current Compliance Issues for Storage Professionals



## **Abstract**

*This report covers recent regulations that mandate how recordkeeping must be performed within a broad range of industries. Becoming in compliance with these regulations will have a significant impact on the storage strategies of organizations around the globe.*

*A dedicated manufacturer of tape storage solutions, GST, Inc. produced this GST Research Report as part of its commitment to provide information leading to the better management of data and application protection within the IT industry.*



### Table of Contents

<b>Forward</b>	4
<b>Executive Summary</b>	5
<b>General Information about Compliance</b>	6
1. What is the background of current compliance issues?	6
2. What was the reaction to corporate scandals?	7
3. What is the concern about privacy?	8
4. What form has compliance regulations taken?	8
<b>Survey of Compliance Regulations</b>	9
5. Sarbanes-Oxley Act	9
6. Health Insurance Portability and Accountability Act (HIPAA)	10
7. Gramm-Leach-Bliley Act	11
8. SEC Regulation 17a-3, 17a-4, 17ad-6, 17ad-7	13
9. NASD 3010 & 3110	14
10. NYSE Rule 440	15
11. Food and Drug Admin: 21 CFR Part 11	17
12. Commodity/Futures Trading: CFTC's 17 CFR Part 1 Regulation 31.1	18
13. Fed. Energy Regulatory Comm (FERC): Part 125	21
14. IRS: Rev Proc 97-22	22
15. Nat. Archives & Records Admin (NARA): Part 1234 & Gen. Rec. Sched 24	24
16. Defense: DOD 5015.2	27
17. Patriot Act	29
<b>Impact of Compliance on Storage Management</b>	30
18. What are the expected impacts on records management within IT?	30
19. What are the requirements of storage media for regulated industries?	31
<b>How to Prepare for Compliance</b>	32
20. How to assure backup media will last the required time period	32
21. How to mitigate against loss of off-site backup data	34
22. How to assure tamper-proof backup media	34
23. How does Mirrored Backup technology aid compliance	35



# GST Research Report

---

## Storage Compliance

Conclusion	36
About the author	36
Feedback	37
About GST, Inc.	37
Trademarks	37



# GST Research Report

---

## Storage Compliance

### Forward

Privacy concerns and recent corporate financial and reporting scandals have awakened the public and sharpened the senses of regulators throughout the United States. The result has been a spate of new regulations aimed at protecting the public's rights in complex financial relationships. In addition, privacy has grown as an issue, particularly in the medical and financial worlds where the privacy rights of patients and investors are being strengthened through new regulations, most notably represented by the new Federal rules to protect patient privacy.

These regulations will have long-ranging effects on the organization and how it manages its records. This, in turn, will strongly affect the way that storage resources are structured and managed. Backup and restore strategies, archiving and disaster recovery will all be affected by the coming wave of new records management and privacy regulations.

With deadlines approaching, and many already here, the compliance issues that storage managers and records management managers face must be thoroughly understood. This understanding of the compliance issues at hand is needed to begin to formulate the best way for each organization to become regulatory compliant in a way that adds rather than detracts from the organization's performance.



## GST Research Report

---

### Storage Compliance

### *Executive Summary*

Recent developments in regulatory rules are having a major impact on records management and storage practices in many industries. Coming from over 10,000 different laws from the U.S. Federal Government and other regulatory agencies, the new mandated rules are affecting storage strategies and backup processes as well as the retention and protection of stored data. Compliance with these regulations is becoming an essential part of any organization's records retention and storage strategy.

Over a dozen new laws and regulations need to be understood for their significant affect on how records management must proceed in the U.S. in the future. Many regulations have already come into effect, others are scheduled to become law in 2004. These laws and regulations are primarily a result of the public's concern over recent corporate scandals in the U.S., terrorism on a global scale, and a growing concern for privacy in a wide variety of areas.

The new regulations will require organizations to store more data in duplicate, store it in an unalterable fashion, and have control procedures in place to prevent it from being altered. Records will have to be retained longer, be indexed and be more searchable in order to furnish records to oversight agencies on demand. All of this will put great pressure on the IT function in 2004 as organizations make the necessary changes to come into compliance.

As a provider of backup solutions, GST has a great interest in all emerging storage issues. Our Mirrored Backup technology and WORM technology products can play a constructive part in assisting organizations to achieve the required levels of compliance that are mandated by the new laws and regulations. Mirrored Backup assures that duplicate copies of important backup data are produced efficiently and mitigates against drive failure jeopardizing backups and restores. Our use of Sony's WORM (Write Once Read Many) technology assures that backup and archive tapes produced on GST dual-drive subsystems and tape libraries are unalterable and non-erasable.

The full report details how the new regulations came about, what they are, their impact on IT and some ways to achieve compliance and reap additional benefits for the organization.



### *General Information about Compliance*

**Note:** In this report, we have used **boldface** to emphasize wording in excerpts to show what is most relevant to IT strategies.

#### 1. What is the background of current compliance issues?

Corporate governance scandals in the energy industry, securities and pharmaceuticals, among others, have been front page headlines. Some of them are:

- Kenneth Lay, CEO, Enron
- Bernard J. Ebbers, CEO, WorldCom
- Martha Stewart, CEO, Martha Stewart Living Omni Media
- Sam Waksal, CEO at ImClone
- Dennis Kozlowski, CEO, Tyco

These and other failures where corporations failed to meet the public trust placed in them resulted in a wave of laws and regulations aimed at different industries. These laws were initially passed in the U.S. Congress and then were expanded upon by various Federal regulatory agencies. These new regulations have prompted organizations to overhaul their storage policies, expand their storage resources and look for ways to save records in a more permanent fashion.

The state and Federal agencies for the financial community alone are shown below.

<b>Federal Agency</b>	<b>Financial Institutions Overseen</b>
Office of the Comptroller of the Currency	National banks, Federal branches of foreign banks and their subsidiaries.
Board of Governors of the Federal Reserve System	Federal Reserve System member banks, foreign banks, bank holding companies and any subsidiaries or affiliates of these institutions.
Board of Directors of the Federal Deposit Insurance Corporation (FDIC)	FDIC insured banks, State branches of foreign banks and their subsidiaries.



# GST Research Report

## Storage Compliance

Federal Agency	Financial Institutions Overseen
Board of the National Credit Union Administration	Any federally insured credit union, and any subsidiaries of such an entity.
Securities and Exchange Commission (SEC)	Any broker or dealer, investment company, or registered investment advisers.
The applicable State insurance authority	Any person engaged in providing insurance.
Federal Trade Commission (FTC)	Any other financial institution or other person that is not subject to the jurisdiction of any agency or authority covered above.

The compliance of organizations with the many government and independent regulatory body laws, rules and regulations has been the subject of many reports and investigations by leading management and IT publications including *CIO Magazine's* series "Playing by New Rules" that began running in April, 2003; see: <http://64.28.79.79/newrules> .

### 2. What was the reaction to corporate scandals?

Both the press and the public exploded with demands to reign in the out-of-control behavior of a few very bad apples in the corporate landscape of the U.S. in 2002 and 2003. Congressional hearings and CNN live coverage further strengthened the cries for strong reforms and harsher penalties for the perpetrators. Enforcement reaction included televised "perp walks" of several prominent executives to arraignment as a result of their alleged violation of existing laws and regulations.

Early investigations encountered a wall of obstacles to getting at the truth of what happened in documentation that would stand up in court. As a direct result of these difficulties to both corporate scandals and the absence of needed evidence, the U.S. Congress passed the Sarbanes-Oxley Act on July 30, 2002. It contains looming deadlines for compliance to a host of records-related regulations, including financial penalties and imprisonment for up to 20 years. According to *Computerworld*, there are now over 10,000 U.S. Federal, state and local laws and regulations that address "what, how, when and why records must be created, stored, accessed, maintained and retained over increasingly longer periods of time."



## GST Research Report

---

### Storage Compliance

#### 3. What is the concern about privacy?

Several concerns have prompted legislation on privacy matters, most notably in the medical records area. First, the devastating hurricanes, floods and fires that have destroyed large segments of communities in the United States in the past five years prompted a need for patient data to be safeguarded and available in the event of such a disaster. Second, the new **Patient's Bill of Rights** includes protection of a patient's medical records from being accessed by those other than the patient's own doctors and family, and prevents insurance companies from accessing patient records to determine what medical insurance they might or might not want to offer (this concern was initially codified in the Patient's Bill of Rights that Congress passed and is a part of every hospital and doctor's office information kit provided to new patients). A third concern is that authentication of those accessing medical records be more tightly controlled in part to prohibit identity fraud. The widespread problem of individuals using other people's security (PIN) numbers to access confidential records like patient charts has resulted in a need to utilize biometrics technology to read fingerprints, voiceprints and face/iris recognition to authenticate the identity of a person before they are granted access to medical records.

#### 4. What form have compliance regulations taken?

Compliance takes many forms. In addition to federal, state and local laws, there are countless rules and regulations within a myriad of oversight organizations including the Securities Exchange Commission (SEC) and New York Stock Exchange (NYSE). These regulations are not concentrated within any one source, and awareness of them is important for IT organizations. Each regulation carries penalties that take the form of non-compliance fines into the millions of dollars per violation plus prison sentences of up to 20 years. Some deadlines for compliance have come and passed, others are still scheduled in the future.



## *Survey of Compliance Regulations*

This section presents basic information about the most widely known and discussed laws and regulations that require compliance to a standard related to the storage of electronic records.

### **5. Sarbanes-Oxley Act**

Enacted August 1, 2002 by the U.S. Congress, the Sarbanes-Oxley Act (SOA) requires changes in financial and corporate reporting to protect investors against poor account practices, accounting errors and fraudulent behavior on the part of investor community organizations. In signing this law, President George Bush said it is, "intended to deter and punish corporate and accounting fraud and corruption, ensure justice for wrongdoers, and protect the interests of workers and shareholders." This act is wide-reaching and affects securities broker-dealers and all companies publicly traded in the U.S. securities markets. Firms with market capitalization above \$75 million have major deadlines coming due in June 2004.

After June 15, 2004, companies covered by the act must have made an effort to comply with the financial reporting disclosure requirements laid down in SOA. Section 404 of SOA, mandates that all registered public accounting firms that prepare audit reports on client financial statements must confirm and report so, that the assessment in the disclosure is accurate. Both the accounting firms and the Corporate CEOs (and by extension, their CFOs and CIOs) must sign a statement that affirms policies and procedures are in place to ensure accuracy in asset disposition, transactions and internal reporting processes.

Besides requiring CEO/CFO certification of internal controls, the act requires documents to be held longer and includes penalties for alteration and destruction of records. For example, fines and imprisonment of up to 20 years are proscribed for any person who "corruptly" alters, destroys or conceals any records or documents to impair the use of them in any investigation. Also, failure to maintain audit/review "workpapers" for at least five years can result in fines or imprisonment for up to 5 years.

*CIO Magazine* surveyed 19 companies on the Fortune 100 list; they found that most executives viewed compliance with the Sarbanes-Oxley Act as a finance issue, not a systems issue. Some organizations acknowledged a possible involvement by IT but they insisted it was premature for the CIO to be involved. The magazine concluded that this view is not only incorrect, but hampers the organization's ability to respond to the challenges of SOA.



## GST Research Report

---

### Storage Compliance

The SEC's own web site has this to say about SOA:

On July 30, 2002, President Bush signed into law the Sarbanes-Oxley Act of 2002, which he characterized as "the most far reaching reforms of American business practices since the time of Franklin Delano Roosevelt." The Act mandated a number of reforms to enhance corporate responsibility, enhance financial disclosures and combat corporate and accounting fraud, and created the "Public Company Accounting Oversight Board," also known as the PCAOB, to oversee the activities of the auditing profession. The full text of the Act is available at <http://www.law.uc.edu/CCL/SOact/soact.pdf>. You can find links to all Commission rulemaking and reports issued under the Sarbanes-Oxley Act at <http://www.sec.gov/spotlight/sarbanes-oxley.htm>.

Compliance: All audit and review information must be retained in a readily accessible and indelible format for seven years. This retention of records for an extended period in a manner that cannot be altered must be in place by June 2004 for public institutions.

Bottom line for IT: SOA defines for IT which types of records must be stored for how long and under what conditions.

Sarbanes-Oxley links:

1. [www.sarbanes-oxley.com](http://www.sarbanes-oxley.com)
2. [www.sarbanes-oxley-forum.com](http://www.sarbanes-oxley-forum.com)
3. [www2.cio.com/analyst/report1537.html](http://www2.cio.com/analyst/report1537.html)
4. [www.cio.com/archive/051503/rules.html](http://www.cio.com/archive/051503/rules.html)
5. [www.darwinmag.com/read/040103/govern.html](http://www.darwinmag.com/read/040103/govern.html)
6. <http://news.findlaw.com/hdocs/docs/qwbush/sarbanesoxley072302.pdf>

### **6. Health Insurance Portability and Accountability Act (HIPAA)**

Enacted by Congress in August 1996, the HIPAA legislation specifies mechanisms for the exchange of electronic data, records confidentiality and security steps that must be in place to maintain confidentiality. HIPAA affects health care providers of all types from the single doctor or store-front medical establishment to large hospital chains. Health care insurers and health claims clearinghouses are also targeted.

The act encourages use of electronic form of records and transactions to improve record keeping efficiencies. Medical records must be maintained for at least 6 years, as well as two years after death. Moreover, it requires health providers to safeguard patient information and to make it available in case of a disaster.



# GST Research Report

---

## Storage Compliance

Section 1173 (d) (2) requires reasonable and appropriate administrative, physical and technical safeguards must be maintained to ensure the integrity of medical-related data. This includes “data authentication” that verifies that data has not been altered, destroyed or inappropriately processed. Clearly, storage will have to become more indelible to comply with these regulations. Penalties for non-compliance include fines up to \$250,000 and up to 10 years in prison.

Experts are advising the IT departments of affected organizations to consider newer storage technologies for longer-term record keeping. They predict that efforts to upgrade storage technology to meet the new HIPAA regulations will improve both productivity and customer service.

Compliance: Compliance with HIPAA requires a comprehensive program within the affected medical community to develop internal policies as well as ongoing training and audits of personnel and practices.

Bottom line for IT: Rules for retention and protection of data in medical industries are already in place. IT needs to move to ensure compliance where internal IT procedures are not in compliance with HIPAA rules and practices.

HIPAA links:

1. [www.HIPAAAdvisory.com](http://www.HIPAAAdvisory.com)
2. [www.hipaa.org/](http://www.hipaa.org/)
3. [www.cms.hhs.gov/hipaa](http://www.cms.hhs.gov/hipaa)
4. [www.cio.com/archive/070103/eight.html](http://www.cio.com/archive/070103/eight.html)
5. <http://aspe.hhs.gov/admnsimp/index.shtml>

### **7. Gramm-Leach-Bliley Act.**

On November 12, 1999 President Clinton signed the Gramm-Leach-Bliley Act (GLBA) into law, spearheaded by Senator Phil Gramm, Chairman of the U.S. Senate Banking Committee. Just as HIPAA focuses on patient and health privacy, GLBA focuses on financial privacy. The law targets a wide variety of financial institutions: banks, credit unions, collection agencies, credit bureaus, check cashing companies, credit counseling organizations, brokers, tax planning and preparation companies, retailers that issue their own credit cards, auto dealers that lease and/or finance, companies that sell money orders and/or travelers checks, investment companies, investment advisors, and insurance companies.

The US Senate recognized that no security begets no privacy. That’s why Senators Gramm, Leach and Bliley authored the data protections of Nonpublic Personal Information in Section 501(b) that were added to the GLBA. These protections are wide-reaching within the financial community and require federal banking agencies, the U.S. Securities and Exchange



## GST Research Report

---

### Storage Compliance

Commission SEC), the Federal Trade Commission (FTC) and the National Credit Union Administration to produce standards regarding the administrative, technical and physical protection of customer data. The federal banking agencies (OCC, FRB, FDIC, OTS and NCUA) have relevant regulations that came into effect in July 2001. Relevant SEC regs also came into effect in July 2001. The FTC's regulations to enforce GLBA came into effect on May 23, 2003. Many affected organizations have not yet come into compliance with these regulations, and are exposed to the penalties attached to each violation.

While not an Internet-specific law, GLBA affects how businesses treat certain financial data in both online and offline formats. Conditions where financial institutions can disclose nonpublic personal information about a consumer to unaffiliated third parties is restricted, and it requires them to disclose certain privacy policies and practices to all of its customers. This has resulted in the proliferation of "Privacy Policy" mailers that financial institutions have mailed to all their customers over the past two years.

The GLBA Data Protection Rule, also called the Information Safeguards Rule (16 CFR Part 314), was published by the FTC in May of 2002. This rule specifies the necessary elements that organizations needed to include in their Comprehensive Information Security Program. As noted, the deadline for the Data Protection Rule was May 23, 2003. This regulation requires organizations to create, implement and maintain a "comprehensive written information security program". This program must contain administrative, technical and physical safeguards to protect customer information. If an organization's existing checks and balances are inadequate, new protective measures will be required. This could lead to a variety of actions including the addition of data encryption, formalizing "need to know" policies, procedures for disposal of trash and old scratched tapes and implementation of access security to file cabinets and desks.

IT and other administrative segments of the organization will either identify, or more likely develop, administrative, physical and technical structures to protect the confidentiality and integrity of personal consumer information. Subtitle A of Title V of the Act says "Institutions must protect against any anticipated threats or hazards to the integrity of such records." Penalties for failure to comply include criminal prosecution, fines and up to five years in prison.

**Compliance:** To initially comply with GBLA, most firms have sent written privacy policies by now to their employees and customers. Fewer organizations have implemented storage strategies to secure and protect customer data according to the criteria set forth in a wide array of rulings and regulations generated by GBLA.

**Bottom line for IT:** Rules for safeguarding the integrity of data for financial institutions focus on security.



# GST Research Report

---

## Storage Compliance

### GLBA links:

1. [www.privacyassociation.org/docs/102\\_ftc-outline.pdf](http://www.privacyassociation.org/docs/102_ftc-outline.pdf)
2. [www.amisgroup.com](http://www.amisgroup.com)
3. [www.bankersonline.com/vendor\\_guru/compcoach/compcoach\\_data.html](http://www.bankersonline.com/vendor_guru/compcoach/compcoach_data.html)
4. [www.epic.org/privacy/glba](http://www.epic.org/privacy/glba)

### **8. SEC Regulations 17a-3, 17a-4, 17ad-6, 17ad-7.**

Regulations enacted by the US Securities and Exchange Commission (SEC) are of significance to many organizations. SEC Rule 17 focuses on the securities industry. Other rulings interpret requirements in Sarbanes-Oxley that apply broadly to public corporations.

In 1997, the SEC enacted regulations 17a-3 and 17a-4, focusing on brokers in the securities industry, allowing them to store records electronically. Rule 17a-3 deals with the establishment of electronic records. Rule 17a-4, passed in May 2001, deals with the requirement of how to keep electronic records. These regulations state that brokers and others in the securities industries must have the following practices documented and in place:

- Written and enforceable records retention policies.
- Data stored on a non-rewriteable and non-erasable media such as WORM (Write Once Read Many).
- Automatic verification of the accuracy and quality of the storage media recordkeeping process.
- Searchable index of all stored data that is downloadable to other formats.
- Readily retrievable and viewable data acceptable by third parties.
- Serialization of original and required duplicate units of storage media.
- Storage of data offsite.

In 2002, financial institutions that were fined \$1.65 million for violations of these rules included: Deutsche Bank Securities, Goldman Sachs, Morgan Stanley, Salomon Smith Barney and U.S. Bancorp Piper Jaffray.

SEC regulations 17ad-6 and 17ad-7 focus on transfer agents. These are organizations that keep shareholder records; issue new certificates; distribute proxies, dividends and annual reports; and forward company correspondence to shareholders. Rule 17ad-6 deals with the requirements for what type of data to store and how long to store it. Some specified time periods for financial and securities industry members:

- Financial statements: 3 years
- Member registration for brokers/dealers: to the end of life of the enterprise
- Trading account records: to the end of the account plus 6 years (included email)



# GST Research Report

---

## Storage Compliance

Rule 17ad-7 has to do with how the data must be stored. Transfer agents are required to comply with the following requirements (exact wording shown):

- "Use storage devices that are designed to ensure the accessibility, security and **integrity** of the records."
- "Detect attempts to alter or remove the records."
- "Provide a means to recover altered, damaged, or lost records."

An American Bankers Assn *Industry Issues* newsletter states:

"The Securities and Exchange Commission (SEC) Rule 17 a-4 (B) (4) requires a three-year retention for all incoming and outgoing communications, including electronic. If there are any state retention schedules that are for a longer period of time, the longer time should be used."

Compliance: see in NASD 3010 & 3110 below.

Bottom line for IT: Rules for storing and protecting electronic records for broker and securities organizations are very specific and mandate new challenges for ensuring permanence of the data within the securities industry.

SEC Rule 17 links:

1. [www.law.uc.edu/CCL/34ActRIs/rule17a-4.html](http://www.law.uc.edu/CCL/34ActRIs/rule17a-4.html)
2. [www.windowfs.com/forum.asp?ID=8](http://www.windowfs.com/forum.asp?ID=8)
3. [www.aba.com/Industry+Issues/QAApril2003.htm](http://www.aba.com/Industry+Issues/QAApril2003.htm)
4. [http://transformmag.com/db\\_area/archs/2003/07/tfm0307br\\_1.shtml](http://transformmag.com/db_area/archs/2003/07/tfm0307br_1.shtml)

### 9. NASD 3010 & 3110.

The National Association of Securities Dealers, Inc. (NASD) is an oversight regulatory group established to review and govern the behavior of firms in the securities industries. In 1997, NASD amended Rule 17a-4 to produce NASD 3010 and 3110, which defined rules pertaining to mandated oversight that each securities dealer must conduct with its registered securities representatives.

Rule 3010 relates to supervision. It states that each securities firm must actively supervise the activities of their representatives, including a process that monitors both incoming and outgoing email messages.

Rule 3110 relates to the retention of correspondence. It states that securities firms must retain all correspondence of their representatives that are part of its securities or



## GST Research Report

---

### Storage Compliance

investment banking business. This rule spells out the requirements for maintaining record keeping, record formats, storage mediums and records retention periods that comply with and support SEC Rule 17a-4 (covered above).

The penalties described above for SEC Rule 17 were also based on NASD 3010 and 3110. These fines totaled over \$8 million for five of the largest investment banks in the world and presage even larger penalties of up to \$500 million for some firms in the future.

A new requirement, published by NASD in a notice to its members on June 18, 2003, says: "Regardless of the informality of instant messaging, it is still subject to the same requirements as email communications and members must ensure that their use of instant messaging is consistent with their basic supervisory and record keeping obligations." This decision follows a similar directive from a recent New York Stock Exchange memo, which states that record retention as outlined by NYSE Rule 440 and SEC Rule 17a-4 applies to instant messages as well as email.

Compliance: Affected firms must accomplish all of the following to be in compliance:

- Thoroughly documented and enforceable records retention policies.
- Data must be stored on indelible, non-rewriteable and non-erasable media.
- A search/reference index must be available for of all stored data
- Data must be readily retrievable and viewable.
- Data must be stored off-site.

Bottom line for IT: Rules for storing and protecting electronic records for securities dealers are specific and mandate new challenges for ensuring permanence of the data within the securities industry.

NASD 3010 & 3110 links:

1. [www.ziplip.com/solutions/compliance.html#SEC](http://www.ziplip.com/solutions/compliance.html#SEC)
2. [www.aungate.com/c/content/compliance/compliance](http://www.aungate.com/c/content/compliance/compliance)
3. [www.complianceweek.com/whitepapers/imlogic.pdf](http://www.complianceweek.com/whitepapers/imlogic.pdf)

#### **10. NYSE Rule 440.**

Basically, this rule by the New York Stock Exchange requires securities brokers and dealers to preserve various types of records as prescribed by the NYSE and by the SEC in Rule 17a. NYSE Rule 440 includes the preservation of electronic messages within the securities industries that relate to the NYSE. As mentioned above, in 2002 each of the securities and dealers associated with the NYSE - Deutsche Bank Securities; Goldman, Sachs & Co.; Morgan Stanley & Co.; Salomon Smith Barney; and U.S. Bancorp Piper Jaffray - consented,



## GST Research Report

---

### Storage Compliance

without admitting or denying the allegations, to findings that each violated the following: Section 17(a) of the Securities Exchange Act of 1934, Rule 17a-4 under the Exchange Act, and **NYSE Rule 440** and NASD Rule 3110 by failing to preserve for a period of three years, and/or preserve in an accessible place for two years, electronic communications relating to the business of the firm, including interoffice memoranda and communications. The SEC website (first reference link below) also makes the following statements regarding how the email records were retained:

"Some firms backed up e-mail communications on tape or other media that was represented as part of a process designed as a disaster-recovery or business-continuity measure, or for another business purpose. However, these firms discarded or recycled and overwrote their back-up tapes and other media, often a year or less after back-up occurred.

Each firm had inadequate procedures and systems to retain and make accessible e-mail communications. While some firms relied on employees to preserve copies of the e-mail communications on the hard drives of their individual personal computers, there were no systems or procedures to ensure that employees did so.

In those instances in which the firms did retain e-mail communications, those communications were often stored in an unorganized fashion on back-up tapes, other media, or on the hard drives of computers used by individual employees. In some instances, hard drives of computers preserving electronic mail communications were erased when individuals left the employment of the firm."

In NYSE Information Memo No. 03-07 (Mar. 5, 2003)

The New York Stock Exchange provided its "guidance" on instant messaging. The NYSE entitled its memorandum "Electronic Logs and Record Retention". In one section, reproduced in its entirety below, the NYSE stated that instant messages are also subject to the record retention requirements of NYSE Rule 440 and SEC Rules 17a-3 and 17a-4:

#### **Record Retention**

Members are reminded that the record retention requirements of NYSE Rule 440 and the Securities Exchange Act Rule 17a-4 apply to the electronic logs maintained in lieu of paper order tickets and reports of execution, which relate to the member's business. In addition, members and member organizations must ensure that all communications whether electronic or otherwise, including but not limited to e-mails, instant messages, and similar communication devices that relate to the firm's business as such must be maintained and retained in compliance with NYSE Rule 440 and SEC Rules 17a-3 and 17a-4. Any records maintained electronically must be in a non-rewriteable, non-erasable format, i.e., **WORM ('Write Once, Read Many')**."



# GST Research Report

---

## Storage Compliance

Compliance: This Rule 440 from the NYSE has created the need for storage solutions to help broker and dealer firms properly manage, search and retain emails relating to the business, while controlling the costs resulting from managing emails.

Bottom line for IT: Rules for storing and protecting emails and instant messaging are now crucial for the broker and securities industry and reach into emails and even instant messaging.

NYSE Rule 440 links:

1. [www.sec.gov/news/press/2002-173.htm](http://www.sec.gov/news/press/2002-173.htm)
2. [www.duanemorris.com/publications/pub1094.html](http://www.duanemorris.com/publications/pub1094.html)
3. <http://groups.yahoo.com/group/cyberia-l/message/46975>

### **11. Food and Drug Admin: 21 CFR Part 11.**

In March, 1997, the Food and Drug Administration (FDA) produced Article 21 CFR Part 11. Part 11 specifically covers electronic records. The FDA states:

“Part 11 regulations provide criteria for acceptance by FDA, under certain circumstances, of electronic records, electronic signatures, and handwritten signatures executed to electronic records as equivalent to paper records and handwritten signatures executed on paper. These regulations, which apply to all FDA program areas, were intended to permit the widest possible use of electronic technology, compatible with FDA's responsibility to protect the public health.”

For all manufacturers regulated by the FDA, 21 CFR Part 11 establishes standards whereby hardcopy documents can be replaced by electronic documents and signatures. Organizations that are affected are those involved with manufacturing, processing and packaging for the food, drugs/pharmaceuticals and biological products industries.

The protection of records is required in an accurate and retrievable form throughout specified records retention periods:

- Food industries – 2 years after release
- Drugs/pharmaceuticals – 3 years after distribution
- Biological Products – 5 years after the end of manufacturing

The regulation specifies that reproductions of the records covered must be kept “in common and portable formats” and “must preserve the original content and meaning of the records”. The demand for common formats and the ability to be easily retrieved just about rules out anything but electronic copies of records.



## GST Research Report

---

### Storage Compliance

Concerns were raised by the regulated industries particularly in the areas of Part 11 requirements for validation, audit trails, record retention, record copying, and legacy systems. In August 2003, the FDA published their "Guidance for Industry", containing a withdrawal of parts of the regulation and statements as follows:

"The FDA is re-examining Part 11, and we anticipate initiating rulemaking to revise provisions of that regulation. To avoid unnecessary resource expenditures to comply with Part 11 requirements, we are issuing this Guidance to describe how we intend to exercise enforcement discretion with regard to certain Part 11 requirements during the re-examination of Part 11. As mentioned previously, Part 11 remains in effect during this re-examination period."

The FDA intends to exercise enforcement discretion for legacy systems, defined as those systems operational before August 20, 1997. Further clarifications are expected from the FDA.

Compliance: Regulations in effect by the FDA for electronic record keeping in its regulated industries since 1997 have been recently affected by an advisory that enforcement will take a very narrow path until further clarifications ensue.

Bottom line for IT: The changing landscape of records retention and maintenance in the food, drug and bio industries will require careful attention to make sure practices are within their Guidance for Industry recently published.

#### 21 CFR Part 11 links:

1. [www.fda.gov/ora/compliance\\_ref/part11/Default.htm](http://www.fda.gov/ora/compliance_ref/part11/Default.htm)
2. [www.fda.gov/cder/guidance/index.htm](http://www.fda.gov/cder/guidance/index.htm)
3. [www.fda.gov/cder/guidance/5667fnl.doc](http://www.fda.gov/cder/guidance/5667fnl.doc)

#### **12. Commodity Futures Trading Commission: 17 CFR Part 1 Regulation 31.1.**

The CFTC's website states:

"The Commodity Futures Trading Commission (CFTC) was created by Congress in 1974 as an independent agency with the mandate to regulate **commodity futures and option markets** in the United States. The agency protects market participants against manipulation, abusive trade practices and fraud. Through effective oversight and **regulation**, the CFTC enables the markets to serve better their important functions in the nation's economy—providing a mechanism for price discovery and a means of offsetting price risk."



## GST Research Report

---

### Storage Compliance

On June 28, 1999, the CFTC published amendments to the CFTC's Regulation 1.31, contained in 17 CFR Part 1. These amendments affect recordkeeping within the futures commodities trading industry to bring them more in line with SEC regulations over the securities industry.

CFTC's change to Regulation 1.31 in 17 CFR Part 1 became effective immediately. Most importantly, it permits the substitution of electronic media or micrographic media for original documents in most cases. Some types of original documents cannot be replaced with electronic and micrographic media: most notably, original written trading cards and order tickets.

It mandates that record keepers retain electronic media or micrographic media of "required records" for five years and that the records be kept "readily available" during the first two years. Regulation 1.31 (a) also provides that all required records be open to inspection by CFTC and DOJ agents.

Moreover, the regulation requires that record keepers "**promptly** provide copies of originals of any required record upon request, and to provide records on electronic or micrographic media **immediately**", recognizing the ability to provide records from electronic media more quickly than when in original document or micrographic form.

If record keepers choose to store all of a particular class of "required records" on electronic storage media, the organization must enter into an arrangement with a Technical Consultant. This is consistent with SEC regulations for the securities industry. The CFTC has stated that its staff will only seek use of the Technical Consultant to access records when the record keeper has shown it is unable or unwilling to meet its regulatory obligations to furnish them.

The CFTC requires that copies of requested records be submitted on Commission compatible machine-readable media (defined by Commission Regulation 15.00 (1)). A number of different media are allowable, including diskettes, magnetic tape, optical disk; e-mail attachments and FTP transmitted files are acceptable where no security concerns exist. To keep up with changing electronic media formats, the Commission has stated that notice of any changes to the list of acceptable reporting media will be available both in writing and on the Commission's web page ([www.CFTC.gov](http://www.CFTC.gov)), and an updated list will be published in the Federal Register.

One other ruling refers to that situation where the organization has commingled Commission-required records with non-Commission-required records. In this case, the record keeper may not deny agents immediate access to any individual electronic or micrographic storage medium while the record keeper reviews the medium for the presence of privileged material.



## GST Research Report

---

### Storage Compliance

Record keepers using electronic storage media must keep available for inspection procedures to access records and indexes maintained on electronic media, or they must place this information in escrow with an independent third party and keep it updated.

Recognizing the futures industry's limited experience with the design or implementation of complex electronic record-keeping systems, the regulation states:

"...the Commission expects that the transition process from paper-based systems to electronic-based systems will involve implementation problems requiring significant adjustments. If the security, reliability, and accessibility of the recordkeeping process are to be protected during this period of learning and adjustment, it is important that record keepers have clear notice of their ongoing obligations under Regulation 1.31. It is equally important that record keepers keep the Commission informed of the experience gained during this period so that the Commission can develop a reliable basis for making necessary adjustments to its rules."

This statement is an excellent example of how IT can maintain a positive relationship with the regulatory agencies with which it must be in compliance.

The Commission's concerns about the security/integrity of records during the transition period from paper documents to electronic or micrographic records generated an additional requirement. Record keepers are required to:

"...maintain **written operational procedures and controls** that would provide accountability over both the initial entry of required records to the electronic storage media and the entry of each change made to any such records. The Commission believes that all record keepers must have and enforce procedures to keep their required records from being altered or destroyed."

In those cases where a non-rewritable/non-erasable format for electronic records is necessary, the Commission agrees that it is the **medium**, not the storage system itself, which must exclusively preserve records in this format. So the medium must provide the Write-Once Read-Many (WORM) capability.

For an organization in the futures and commodities industry that has not automated its recordkeeping, the most salient aspects of Regulation 1.31 are:

- Show that recordkeeping meets pertinent regulatory requirements before converting it to electronic records.
- Create a duplicate of both required records, an index of those records, and maintain the duplicate at a separate location.
- Have an auditable system for transferring records to electronic media.
- Ensure Commission has the information needed to access electronic records.



## GST Research Report

---

### Storage Compliance

- Provide an independent source for downloading records that are kept solely on electronic media.

The Commission's enlightened attitude toward the use of IT is evidenced in its statement regarding Regulation 1.31, saying it allows "record keepers the flexibility to maximize the cost reduction and time savings available from improved storage technology while continuing to provide Commission auditors and investigators with timely access to a reliable system of records."

Compliance: see section 9. NASD 3010 & 3110.

Bottom line for IT: Although the CTFC is very sensitive to the difficulties of the futures and commodities industry converting from paper to electronic record keeping, it has laid out clear rules that are very similar to Rule 17 of the SEC for the securities industry.

17 CFR Part 1 Regulation 31.1 links:

1. [www.ctfc.gov](http://www.ctfc.gov)
2. [www.ctfc.gov/foia/fedreg01/foi011023a.htm](http://www.ctfc.gov/foia/fedreg01/foi011023a.htm)
3. [www.ctfc.gov/opa/press99/opa4266-99-attch.htm](http://www.ctfc.gov/opa/press99/opa4266-99-attch.htm)

### 13. Fed. Energy Regulatory Commission (FERC): Part 125

The FERC 125 is a regulation published by the Federal Energy Regulatory Commission (FERC) under the Federal Power Act and Natural Gas Act.

It establishes specific retention periods for records kept by public utilities industry organizations and their licensees and by organizations they acquire. Specifically **Part 125** applies to "all books of account and other records prepared by or on behalf of the public utility or licensee."

Part "c" of **Section 125.1 - Protection and Storage of Records** states that protection is required "from fire, floods, and other hazards and in the selection of storage space, safeguards the records from unnecessary exposure to deterioration" from various specified conditions. Further, software and hardware that is required for the retrieval of stored data must be maintained for the retention periods specified in Section 125.3 – Retention Periods; some examples:

- Annual reports: 5 years
- Meeting minutes related to stockholders: 5 years (with conditions)
- Titles, franchises, licenses: 6 years (with conditions)
- Procurement agreements: 6 years
- General accounting ledgers: 10 years



## GST Research Report

---

### Storage Compliance

- Plant ledgers: 25 years

This ruling applies to all forms of records, including email which is highly unstructured. In fact the FERC was looking for ENRON's email records in the highly-publicized investigation that ultimately brought down both ENRON and their auditors Arthur Anderson. You don't have to be guilty of anything to be forced to respond to a request for records from the FERC. A number of West Coast energy companies were forced to respond to similar investigations by FERC during the California energy crisis of 2001.

Compliance: Regulations are now in effect and compliance is mandatory.

Bottom line for IT: Records retention is crucial in the utilities industries, with 42 different kinds of records specified, each with its own retention period.

FERC Part 125 links:

1. [www.hoovers.com/free/co/factsheet.xhtml?COID=116512](http://www.hoovers.com/free/co/factsheet.xhtml?COID=116512)
2. [www.ferc.gov/default.asp](http://www.ferc.gov/default.asp)
3. [http://a257.g.akamaitech.net/7/257/2422/14mar20010800/edocket.access.gpo.gov/cfr\\_2002/aprqrtr/pdf/18cfr125.2.pdf](http://a257.g.akamaitech.net/7/257/2422/14mar20010800/edocket.access.gpo.gov/cfr_2002/aprqrtr/pdf/18cfr125.2.pdf)

#### **14. IRS: Rev Proc 97-22.**

The Internal Revenue Service (IRS) has published IRS Revenue Procedure 97-22 to provide guidance and guidelines for the maintenance of electronic records pertaining to tax filings. It applies to all taxpayers and tax paying organizations.

**Part 03 Section 1.6001-I (e) of Rev Proc 97-22** states:

"...the books or records required by Section 6001 must be kept available at all times for inspection by authorized Internal Revenue Service officers or employees, and must be retained so long as the contents thereof may become material in the administration of any internal revenue law."

Note there is no specific retention period given other than the vague guideline at the end of the above quote.

**Section 4 Electronic Storage System Requirements** stipulates that the electronic storage system used must meet the following requirements:

- Ensure the integrity and accuracy and reliability of information stored.



## GST Research Report

---

### Storage Compliance

- Prevent any type of alteration to the records, as well as prevent deletion or deterioration of stored electronic records.

The electronic records that this regulation applies to can be either electronic images of hardcopy forms, or they can be electronic records that contain the data from such forms.

The taxpaying organization must retrieve and produce electronic or hardcopy data when ordered to do so by the IRS. Further, the IRS must be provided the resources (hardware, software, personnel) to locate, retrieve, read and copy any records located anywhere. There must be no restriction to the IRS' access to the storage system used to hold electronic tax records.

If tax records are stored electronically in a medium where the hardware or software is no longer available to access the data, the data is considered destroyed by the IRS.

**Section 11 Paperwork Reduction Act for Rev Proc 97-22** gives the IRS's own estimate of the annual burden on record keeping as a result of this regulation:

- Total annual record keeping burden: 1,000,400 hours
- Annual burden per record keeper: range is 20 to 22 hours, average is 20
- Total number of record keepers this applies to: 50,000

The IRS District Director can, at its choosing, conduct tests of an organization's electronic record keeping system, including hardware, software, indexing procedures, and how documents are stored and reproduced electronically. The internal controls, security procedures and documentation are also subject to this review.

Penalties for non-compliance can be severe. **Section 8 Impact on Machine-Sensible Records**, states;

"The District Director may issue a Notice of Inadequate Records pursuant to Section 1.6001-1 (d) if the taxpayer's books and records are available only as electronically stored books and records and the taxpayer's electronic storage system fails to meet the requirements of this revenue procedure. Taxpayers whose electronic storage system fails to meet the requirements of this revenue procedure may also be subject to applicable penalties under subtitle F of the Code, including the Section 6662(a) accuracy-related civil penalty and the Section 7203 willful failure criminal penalty."

Compliance: Electronic records related to tax filings must be retained by all individuals and organizations filing a tax return with the IRS, and those records must be kept as long as they are material to the IRS Tax Code.



## GST Research Report

---

### Storage Compliance

Bottom line for IT: District Directors can test record keeping hardware, software, procedures, documentation and controls for electronic tax records at any time and all equipment, software, data and procedures must be available for IRS agents to personally inspect.

IRS Rev Proc 97-22 links:

1. [www.recapinc.com/irs\\_97-22.htm](http://www.recapinc.com/irs_97-22.htm)
2. [www.intltaxlaw.com/INBOUND/reporting/rp9722.htm](http://www.intltaxlaw.com/INBOUND/reporting/rp9722.htm)
3. <http://moneycentral.msn.com/content/Banking/P50242.asp>
4. [www.taxanalysts.com/www/readingsintaxpolicy.nsf/0/A3AC2E2AE5A7E52F85256B82008065EB?OpenDocument](http://www.taxanalysts.com/www/readingsintaxpolicy.nsf/0/A3AC2E2AE5A7E52F85256B82008065EB?OpenDocument)

#### **15. Nat. Archives and Records Admin (NARA): Part 1234 and GA Schedule 24.**

The National Archives and Records Administration (NARA) is an independent Federal agency that preserves United States history and oversees the management of all Federal records. In a statement by John Carlin, Archivist of the United States, before the U.S. House *Subcommittee on Technology Policy, Information Policy, Intergovernmental Relations, and the Census of the Committee on Government Reform* on July 8, 2003, he said:

“NARA is responsible for preserving and providing sustained access to records of all three branches of the Federal Government. We share the common challenge entailed by rapid changes in the technology. This challenge is two-edged: On the one side, rapid obsolescence makes it difficult to maintain old hardware, software, and digital formats; on the other, progress in technology offers better solutions that offer the possibility of improving service to customers. In NARA's case, this challenge is magnified by the need to preserve and deliver authentic records for generations of Americans who will not be born for a hundred years or more.”

“NARA alone is mandated to provide ready access to essential records of what the Federal Government does—why, how, and with what consequences.”

NARA's authority comes from the Code of Federal Regulations (CFR). Subchapter B on Records Management in the CFR covers parts 1220 – 1238, all on records management. Subpart C of Part 1234 is on *Standards and the Creation, Use, Preservation and Disposition of Electronic Records* and includes the following Sections:

- 1234.20 Creation and use of data files
- 1234.22 Creation and use of text documents
- 1234.24 Standards for managing electronic mail records
- 1234.26 Judicial use of electronic records
- 1234.28 Security of electronic records



# GST Research Report

---

## Storage Compliance

- 1234.30 Selection and maintenance of electronic records storage media
- 1234.32 Retention and maintenance of electronic records
- 1234.34 Destruction of electronic records

**NARA Part 1234 Section 1234.22 - Creation and Use of Text Documents** states that any electronic record keeping system that maintains the official copy of a document on electronic media must meet the following criteria:

- Provide a search method for retrieving a desired document.
- Provide security to ensure integrity of the documents (elaborated on in Section 1234.28).
- A standard interchange format to permit the exchange of documents between agency computers.
- Provide disposition of the document, i.e., mandatory retention periods.

**Section 1234.28 - Security of Electronic Records** requires the following practices:

- Permit only authorized personnel access to electronic records.
- Backup and recovery of records provided to protect against information loss.
- Train appropriate agency personnel to safeguard sensitive or classified electronic records.
- Minimize the risk of unauthorized alteration or erasure of electronic records.

**Section 1234.30 - Selection and Maintenance of Electronic Records Storage Media** contains numerous requirements related to storage media; a representative list includes:

- Permit easy retrieval in a timely fashion.
- Keep records in a usable format until their authorized disposition date.
- Before conversion to a different medium, determine that the authorized disposition of the electronic records can be implemented after conversion.
- Back up electronic records on a regular basis to safeguard against loss of information due to equipment malfunctions or human error. **Duplicate copies** of permanent or unscheduled records shall be maintained in storage areas separate from the location of the records that have been copied.
- Test magnetic computer tapes no more than 6 months prior to using them to store electronic records that are unscheduled or scheduled for permanent retention.
- Annually read a statistical sample of all computer tapes containing permanent and unscheduled records to identify any loss of data and to discover and correct the causes of data loss.
- Before magnetic tapes become 10 years old, copy permanent or unscheduled data stored on them onto tested and verified new tapes.



# GST Research Report

---

## Storage Compliance

**Section 1234.32 - Retention and Disposition of Electronic Records** has these standards worth noting:

- Disposition of electronic records, documentation and indexes is to be scheduled by applying General Records Schedules (particularly GRS 20 or GRS 23) as appropriate or submitting an SF 115, Request for Records Disposition Authority, to NARA.
- Disposition of information in electronic information systems, *including those operated for the Government by a contractor*, is to be identified and scheduled not later than one year after implementation of the system.
- Procedures must be established for recopying, reformatting, and maintenance of electronic records to ensure their retention and usability up to their point of disposition (which can easily be 10 or more years).
- Electronic mail records may not be deleted or otherwise disposed of without prior disposition authority from NARA (44 U.S.C. 3303a). This applies to the original version of the record that is sent or received on the electronic mail system and any copies that have been transferred to a record keeping system.

NARA also maintains their **General Records Schedule 24 - Information Technology Operations and Management Records**. This is a schedule of record retention periods that provide disposal periods for specified files created and maintained in the running and management of information technology (IT) operations and related services. Note these rules pertain to the operation of the IT function and not to normal data records used by applications.

Although most periods for records in Schedule 24 are from 1 to 3 years, there are two specifications that should be singled out for attention: sections 6 and 11.

**Section 6 - User Identification, Profiles, Authorizations, and Password Files** states that internal IT record keeping systems requiring special accountability, e.g., those containing information that may be needed for audit or investigative purposes and those that contain classified records must be retained for 6 years after the user account is terminated or password is altered, or until no longer needed for investigative or security purposes, whichever is later.

**Section 11 - IT Infrastructure Design and Implementation Files** states "Records of individual projects actually implemented that were designed to provide and support new agency IT infrastructure, systems, and services" must be retained 5 years after project is terminated.

Compliance: NARA regulations affect all Federal government record keeping practices and are very specific about electronic record keeping. All are in effect now and have been adopted by some states and other agencies and contractors outside the Federal government.



# GST Research Report

---

## Storage Compliance

Bottom line for IT: If you are involved with Federal electronic records, the rules are clearly spelled out in Part 1234 Sections 20 through 34 and in General Records Schedule 24.

NARA Part 1234 links:

1. [www.archives.gov/about\\_us/regulations/part\\_1234.html#partc](http://www.archives.gov/about_us/regulations/part_1234.html#partc)
2. [www.archives.gov/records\\_management/records\\_schedules.html](http://www.archives.gov/records_management/records_schedules.html)
3. [www.archives.gov/records\\_management/ardor/index.html](http://www.archives.gov/records_management/ardor/index.html)
4. <http://www.archivists.org>

### **16. Department of Defense: DoD 5015.2.**

DoD regulation 5015.2 is part of the Department of Defense (DoD) Records Management Program. Re-issued June 19, 2002, it was developed for DoD by the National Archives and Records Administration – NARA (see 15. above) and provides mandated standards for electronic record management systems that must be provided by Records Management Applications (RMA) purchased by a Federal agency.

L. Reynolds Cahoon, Assistant Archivist for Human Resources and Information Services and CIO for NARA stated on July 8, 2003 before the U.S House *Subcommittee on Technology Policy, Information Policy, Intergovernmental Relations, and the Census of the Committee on Government Reform*:

“NARA has made substantial contributions to the development and the success of the DoD standard for Records Management Applications (DoD 5015.2-STD), the *de facto* standard for records management software, adopted by private companies, as well as by other governments, such as the State of Michigan. Currently there are over 40 commercial off-the-shelf software products certified as compliant with the Department of Defense standard. And NARA is supporting DoD in its efforts to update and enhance this standard.”

DoD 5015.2 contains a description of the scope of this ruling:

“This Directive applies to the Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities of the Department of Defense.” These groups collectively are known as the DoD Components.



## GST Research Report

---

### Storage Compliance

**Section C2.2.9 – Systems Management Requirement** has several regulations worthy of attention:

**C2.2.9.1 Backup of Stored Records** – states that the RMA must automatically create backup or redundant copies of the records and their metadata.

**C2.2.9.2 Storage of Backup Copies** – requires that the method for backing up database files must provide copies of data records and their metadata that can be stored off-line at separate locations to prevent loss due to system failure, operator error, natural disaster or willful destruction.

**C2.2.9.4 Rebuild Capability** – required the RMS to be able to rebuild from any backup copy, using the backup copy and all subsequent system audit trails.

**C2.2.9.5 Storage Availability and Monitoring** – requires the RMA to monitor available storage space. Storage stats must detail the amount of storage consumed by the RMA. Notice of critically slow storage space must be provided by the RMA.

**C2.2.10.2 External E-mail** – One records management ruling that must be implemented by the organization using the RMA is that the user organization must implement procedures to enable e-mail records to be managed by the RMA if that capability is not already part of the RMA. Records retention rules apply to e-mail as much as any other form of electronic records. Managing the retention of e-mail instant messages is a significant challenge, since they were not designed for records management.

Compliance: This standard came immediately into effect in June 2002 and is mandatory for all DoD Components.

Bottom line for IT: If you are in the Federal government or working with DoD, you should be following these regulations.

DoD 5015.2 links:

1. [www.dtic.mil/whs/directives/corres/pdf/50152std\\_061902/p50152s.pdf](http://www.dtic.mil/whs/directives/corres/pdf/50152std_061902/p50152s.pdf)
2. [www.dtic.mil/whs/directives/corres/pdf/d50152\\_030600/d50152p.pdf](http://www.dtic.mil/whs/directives/corres/pdf/d50152_030600/d50152p.pdf)



## GST Research Report

---

### Storage Compliance

#### 17. Patriot Act

The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act, or simply Patriot Act) was enacted by Congress on October 16, 2001. It grants the U.S. Justice Department new surveillance powers. One part is aimed at money laundering among all U.S. organizations by putting procedures and policies in place to detect and to prevent money laundering. The Patriot Act also covers detection of terrorism, immigration violations and discrimination.

Strict reporting requirements are specified for financial institutions, and Section 215 of the Patriot Act amends the Foreign Intelligence Surveillance Act of 1978 to permit certain Federal agencies to have much greater access to an organization's confidential data. Section 215 authorizes federal representatives to:

"... make an application for an order requiring the production of any tangible things (including books, records, papers, documents and other items) for an investigation to protect against international terrorism or clandestine intelligence activities."

The act permits use of court orders to obtain confidential data in those cases where there is only a belief that an individual or organization may have any relevance to a criminal investigation. And it prevents anyone from disclosing that the FBI has requested such data. This data can then be shared by the FBI with other agencies under the Homeland Security bill passed in 2002 that states the FBI must share its data with other law enforcement agencies. Although legal challenges to the act exist, it is the law of the land.

*CIO Magazine* has been quoted as stating, "It is up to the CIO, as the keeper of data, to make sure his company is not fined by the feds or sued by its customers." This most clearly applies to the Patriot Act, where the stigma of a ruined reputation is as great as any fines imposed for non-compliance.

Compliance: Response to requests for data from Federal agencies must be within five days.

Bottom line for IT: Must be able to extract and furnish recordings of messages within parameters specified by the requesting agency. Also, may be required to install name-scanning software to prevent transactions like bank transfers from occurring for a named individual and to report that transaction promptly to the agency.

Patriot Act links:

1. [www.cio.com/archive/041503/data.html](http://www.cio.com/archive/041503/data.html)
2. [www.epic.org/privacy/terrorism/hr3162.html](http://www.epic.org/privacy/terrorism/hr3162.html)
3. [www.fas.org/irp/crs/RS21203.pdf](http://www.fas.org/irp/crs/RS21203.pdf)
4. <http://news.findlaw.com/cnn/docs/terrorism/hr3162.pdf> see Title II, Sec 209, 210



## ***Impact of Compliance on Storage Management***

### **18. What are the expected impacts on records management within IT?**

Here is GST's list of how records-management legislation is affecting IT:

1. **Different retention periods** – Numerous different retention periods are mandated in a multitude of regulations.
2. **Longer retention periods** – Retention periods have been extended, and sometimes the period isn't easy to determine in advance (i.e., HIPAA says keep records 2 years past a patient's death, IRS says keep them *as long as necessary* to stay in compliance with the Tax Code).
3. **Non-erasible records** – The new requirement for non-alterable and non-erasable records will affect the type of media used; almost certain to be satisfied by WORM (write once read many) technology.
4. **Fraud detection** – The new requirement to report when an attempt to modify or delete a record has occurred; this will require strengthening procedures affecting all electronic records.
5. **Better controls** – Requirement for increased internal control over the operation of the IT function to provide greater access security and detailed record keeping of actions dealing with backup files; records retention controls and procedures must be documented in an auditable fashion.
6. **Duplicate data** – Requirement to maintain duplicate backup data sets off-site; this will affect labeling, which needs to be identical as well.
7. **e-mail** – Requirement to place e-mail and Instant Messaging functions under records management control.
8. **Response time** – Requirement to respond quickly to furnish information in a variety of formats to requesting Federal agencies and to ensure agency personnel have access to all parts of the records management system including commercial data centers.



## GST Research Report

---

### Storage Compliance

9. **Technical challenge** – Requirement to maintain and retrieve records for up to 30 years. Since both media and hardware to read and write electronic records is constantly evolving, this presents technical challenges.
10. **Surveillance via IT** – Requirement to implement surveillance procedures when requested to do so under the Patriot Act.
11. **Ever-changing** – Many of the regulations are admittedly interim rulings until further clarifications are published and must be constantly monitored.

#### **19. What are the growing requirements of storage media for regulated industries?**

Compliance with requirements that are faced by broker-dealers in the securities industry can serve as a useful example. The securities industry has been the focus of much legislation to minimize the possibility of fraud or mismanagement that leads to investor loss. Four of the mandated requirements with the greatest impact on IT are described below.

##### **Non-erasable Storage**

Messages must be preserved in WORM (Write Once Read Many) format. Both normal e-mail records and Instant Message type e-mails must be archived on WORM-based media for no less than 2 years, and no more than 6 years.

##### **Mandated Archiving and Duplication**

The initial communications and its corresponding details such as date/time of transmission must be archived and identified with a serial code number. The logging of the specific time and date of original transmissions cannot be altered and must remain fixed to the archived message whenever it is retrieved from storage.

##### **Indexing and Retrieval**

The capacity must exist to easily download indexes and records stored on electronic media in a required format. Search and retrieval services should include an ability to state a question, give logical operators or regular expressions like those Internet search engines use. Extractions of records or data in records must be “readily available” for the SEC and NASD when requested, and the indexes must be able to retrieve referenced information.

##### **Verifiable Storage Processes**

The accuracy of the process for storing electronic records on media must be verifiable. The hardware and software system for logging and storing records has to satisfy the rules of audit and supervision described in NASD 3010. The SEC or NASD can require firms to prove the accuracy of the electronic record saving process.



## *How to Prepare for Compliance*

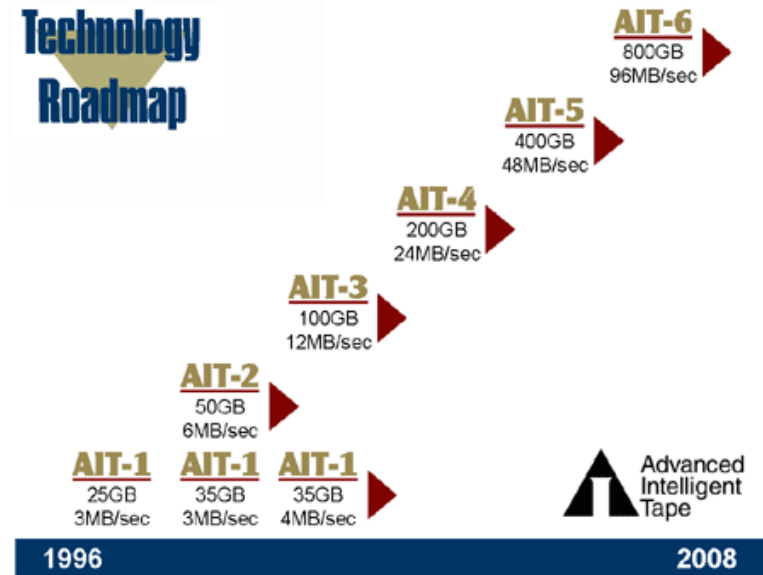
GST has been in the middle of the storage compliance issue ever since the company was founded. A number of the company's solutions contribute directly to achieving compliance with the regulations discussed in this report.

### **20. How to assure that backup media will last the required time period.**

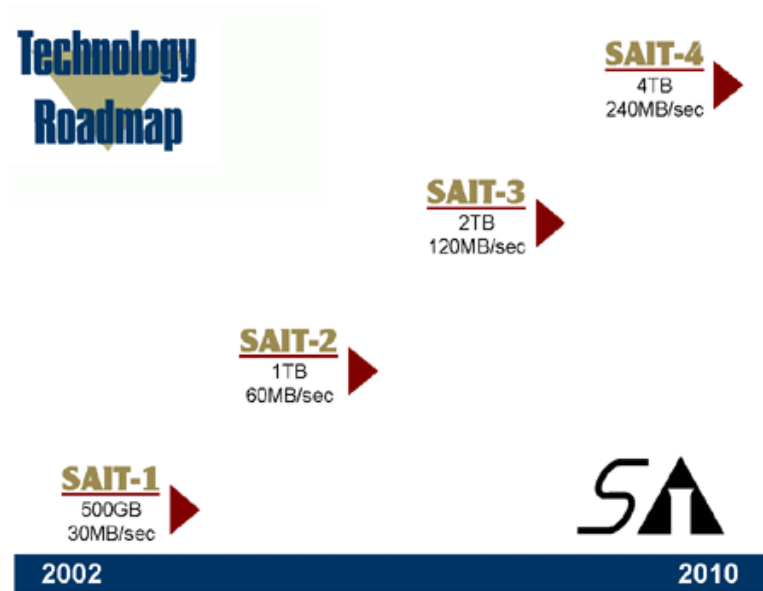
There are some basic ways to make sure that electronic media will be able to remain accurate and usable for the required retention period:

1. **Conduct careful storage** – Store the media in accordance with manufacturer specifications, which are usually significantly more tolerant than the specs listed in NARA or other Federal regulations. The AME tape media used in Sony's AIT (Advanced Intelligent Tape) and S-AIT (Super-Advanced Intelligent Tape) drives has a demonstrated shelf-life of 30 years or more. See Sony's web page on their AME tape media for additional specifications: [www.aittape.com/amemedia.html](http://www.aittape.com/amemedia.html). GST provides tape solutions with AIT and S-AIT technologies that use AME tape cartridges.
2. **Plan for media conversion** – Periodically, electronic media can be converted to a newer electronic record technology. As NARA 1234 states: "Before magnetic tapes become 10 years old, copy permanent or unscheduled data stored on them onto tested and verified new tapes." Tape technologies are continuously evolving, however, the drives themselves are lasting longer. GST's latest tape drive heads have an MTBF (mean time before failure) of 300,000-400,000 hours with a 100% duty cycle. Yet tape technology is improving so fast that typical backup drives are replaced every three years with newer drive technologies featuring more capacity, faster transfer times and greater reliability. This conversion process must be carefully documented and auditable to remain in compliance.
3. **Choose enduring technology** – All tape technologies are not the same when it comes to enduring over extended time periods. The orphaning of archived backup data due to obsolescence of hardware and software is a real problem when retention periods reach out 10-20-30 years. The roadmap for a tape technology is one way of looking at how long a technology might be around. The technology roadmaps for Sony's AIT and S-AIT tape technologies are shown below. AIT is still a young technology with much room for growth, and with technology roadmaps projected out to 2007. It will last much longer, mitigating against unnecessary technology switches and the resulting work it generates for IT.

### AIT Roadmap



### s-AIT Roadmap





## GST Research Report

---

### Storage Compliance

#### **21. How to mitigate against loss of off-site backup data.**

One way to ensure that data remains around for long periods of time is to store more than one copy of it. Each copy should be safeguarded in a separate location. GST's Dual Drive tape backup subsystems using GST's Mirrored Backup technology (see 23 below) produce identical sets of backup cartridges. The duplicate backup copies satisfies those regulatory requirements where maintenance of duplicate backup sets is mandated, and it increases the likelihood that 30 years later the cartridges will remain usable. This approach has the advantage of keeping one backup set readily available for rapid restores, while maintaining the other set at or near the disaster recovery site to facilitate quick recoveries when the main server site is compromised.

#### **22. How to assure tamper-proof backup media.**

SEC regulations 17a-3, 17a-4, 17ad-6, 17ad-7 are most specific about tamper-proof electronic records. Section 17a-4(f)(2)(ii)(A) states that electronic storage media must: "preserve the record's exclusivity in a non-rewritable, non-erasable format." Section (iii)(B) states that this requirement is needed "to ensure that electronic records are capable of being accurately reproduced for later reference by maintaining the records in unalterable form."

The Write Once Read Many (WORM) functionality developed by Sony for AIT and S-AIT tape technology and available in GST tape solutions is ideal for meeting the SEC 17a-4 requirement for tamper-proof media. Sony's WORM Web page states:

"When used with specially marked AIT-2 WORM and AIT-3 WORM media, AIT-2 and AIT-3 drives allow for non-rewritable, non-erasable electronic data storage. In addition to delivering traditional benefits, AIT-2 and AIT-3 drives are backward compatible, with AIT-3 drives fully supporting AIT-1, AIT-2 and AIT-3 rewritable cartridges, as well as AIT-2 and AIT-3 WORM media, and AIT-2 drives fully supporting AIT-1, AIT-2 rewritable cartridges, as well as AIT-2 WORM media. Once recorded, AIT WORM media cannot be re-written or re-formatted, but data can be appended. With the added WORM capabilities, AIT-2 and AIT-3 drives, along with WORM media, will eliminate accidental or intentional erasure of data, enable time and date authentication, and facilitate quick search and retrieval of archived files for a variety of organizations.

GST's AIT WORM products are designed to meet U.S. Securities and Exchange Commission (SEC) regulatory safety, security and integrity requirements. WORM technology provides an ideal storage solution for users in such industries as financial, securities, medical, food, biotech, insurance, federal agencies and firms that desire an extra level of protection for their archived data.



## GST Research Report

---

### Storage Compliance

#### **23. How does Mirrored Backup technology aid compliance?**

Mirrored Backup technology makes duplicate backup sets available to meet regulatory requirements for duplicate archived data sets. It also provides an added measure of protection for data retained over longer periods such as 10, 20 or 30 years.

Mirrored Backup works the same for GST's stand-alone dual-drive mirrored tape subsystems as it does for a GST tape library with two drives. The GST Commander Controller contains logic that enables any dual-drive GST tape subsystem or library to simultaneously produce identical sets of backup cartridges.

The GST tape controller places no extra burden on the server to produce identical, duplicate backup sets. There is no overhead software and no performance degradation to do this. One set of backup tapes can be retained on-site to more quickly initiate the restore process. The other set of backup tapes is transported to a secure remote site that can either be a disaster-proof vault or a Disaster Recovery Center, to be used in the case of catastrophic failure of the IT center.

GST's Mirrored Backup technology also provides a fail-safe capability to the backup process. In the event of a drive failure, GST's Commander tape controller will continue to operate the second drive, ensuring the backup or restore operation is completed successfully. In a long backup, or an even longer restore operation, the ability to avoid having to start over due to a failure near the end of the backup or restore process can be the difference between getting back online within an acceptable time or not ... and not completing a backup or restore within planned limits can be very costly.

GST dual-drives and tape libraries with Mirrored Backup support these tape technologies:

- Sony Advanced Tape Technology: AIT1, AIT2 and AIT3
- Sony Super Advanced Tape Technology: S-AIT1
- Linear Tape Open: LTO1 and LTO2
- Quantum Super DLT
- Tandberg SLR60 and SLR100



## GST Research Report

---

### Storage Compliance

#### Conclusion

In over 10,000 separate regulations, legislative bodies and commissions are mandating that the IT bodies within organizations begin to maintain electronic records in very specific ways. Longer periods of retention are spelled out in detail; electronic records must be stored in safer places and indexed to allow for flexible retrieval, extraction and presentation. In many cases, IT management must ensure that records have been archived in a non-erasable, non-corruptible format and that data was captured in an authentic manner using a regulation-compliant storage system. All data must be available quickly to regulators on demand no matter where it is located.

Failure to comply with these regulations can result in severe penalties that have ranged into the millions of dollars, result in prison sentences of up to 20 years and do permanent damage to an organization's reputation within its markets and the business community.

The good news is that compliance with these regulations can bring additional benefits including improved backup and archival functionality, better financial reporting, improved internal controls and greater access to backup and archived data.

Sony's WORM technology implemented on Sony's AIT and S-AIT drive technology used in GST backup solutions assures the indelible nature of recorded data. This tape technology has a tested shelf life of over 30 years when stored under conditions that are consistent with those in Federal guidelines.

Duplicate backup sets created with GST's Mirrored Backup technology help to meet a number of regulations dealing with assuring the safety of stored data for the required retention periods; they permit local access to one backup set while storing the second backup set in a remote location.

With many regulations already in place and others coming due in 2004, developing a compliance strategy should be a top priority on IT agendas in 2004.

# # #



# GST Research Report

---

## Storage Compliance

### About the author

This GST Research Report was prepared under the leadership of David Breisacher, CEO/Chairman at GST. In addition to founding GST, David has founded several other successful companies including BCC Technologies, a manufacturer of eServer disk, tape and memory storage devices. A visionary for the storage industry since the early 90's, David's market insights and predictions for the storage marketplace are impetus for the research conducted at GST. His experience at structuring backup strategies for hundreds of organizations to meet their data protection needs uniquely qualifies David as the author of this paper.

### Feedback

We value your feedback on this GST Research Report. Please send your comments, suggestions and questions to: [research@gstinc.com](mailto:research@gstinc.com).

### About GST, Inc.

GST Inc. engineers, manufactures, markets and sells a full line of innovative storage backup and restore products to meet today's need for high-performance, fail-safe reliability and cost-effective data storage. Solutions support a wide variety of servers. GST's advanced tape solutions focus on improved backup/restore processes and enhanced disaster recovery. Products range from single and dual tape subsystems and autoloaders to midrange tape libraries and modular enterprise-wide libraries. Unique modular design enables field upgrades, scalability, investment protection and lower life-cycle costs. Development is guided by expert advisory boards that closely track market needs and ensure use of the latest engineering technology in product design. Complete information about the company, its products and support can be found at: [www.gstinc.com](http://www.gstinc.com)

### Trademarks

GST, InternalDR, EntryDR, SafeDR, AutoDR, GrowthDR, ScalableDR, Commander, BridgeLink, SanMatrix and StorMount are trademarks of GST, Inc. in the United States and other countries. All other trademarks and registered trademarks are the property of their respective owners.