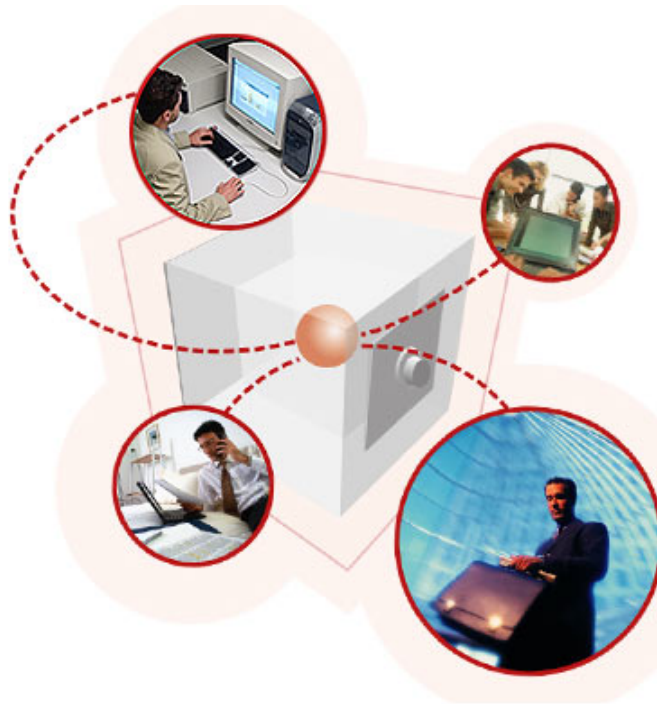


# Critical Practices for Remote Backup



### ***Abstract***

*The protection of the enterprise's data that is stored in far-flung office locations presents unique challenges to the IT organization. This paper explores those challenges and recommends practices that better safeguard data generated at remote sites far away from the IT Department.*

*A dedicated manufacturer of tape storage solutions, GST, Inc. produced this GST Research Report as part of its commitment to provide information leading to improved safeguarding of mission-critical applications and data within the IT industry.*



### Table of Contents

<b>Executive Summary</b>	3
Introduction	4
1. Let the restore process drive the backup	5
2. Clear remote backup procedures	5
3. Use of an operator panel	6
4. Expanded capacity with dual drives	7
5. Mirrored backups with dual drives	8
6. Expanded capacity with autoloaders	9
7. Backup over the Internet	10
8. Take advantage of tape management systems	10
9. Importance of reliability	11
10. Importance of durability	12
11. Importance of repair time	12
12. Get data off your premises quickly	13
13. Key technical concerns	13
14. Give the person backing up the system proper authority	14
15. Compliance issues	14
Feedback	16
Related GST Research Reports	16
About the authorship of this paper	16
About GST, Inc.	16
Trademarks	16



# GST Research Report

---

## Remote Backup

### *Executive Summary*

Today's decentralized IT strategies can result in many remote locations where IT transactions are generated, stored and reported to the central database at IT headquarters. A wide variety of backup devices and network connections are used to attach remote sites to the home IT site. Some of these can transfer backup information, but in many cases the backups are done locally and the backup media is then shipped to the central IT location.

Care must be taken to clearly document and safeguard the backup procedures at remote locations. This documentation must include corrective action to take when backups or restore operations fail for any reason.

The more complete the instructions are for the remote backup operator, the better they can perform their job of completing a successful backup every time. Complete status information about the backup device is critical in assisting the remote operator and centralized tech support professionals to troubleshoot malfunctions and failed backups.

Proper remote backups may require complex backup strategies if the data is to be backed up remotely from the central IT site. Local data protection scenarios can be complex too, and require a thorough understanding of backup options and which approaches are best under a variety of circumstances

The importance of understanding the concepts presented here is to ensure that top management supports the development of data protection strategies that contain the necessary depth to withstand a wide range of threats to the enterprise's critical information resource. The need for such a capability is well-understood by Risk Managers today, and only ignored at the organization's peril.

An enterprise's data is now considered one of its most critical assets. Even the loss of essential data for as little as a few days can result in the eventual failure of the business, as documented in the aftermath of the first World Trade Center bombing on February 26, 1993.

Recent federal, state and local legislation in the U.S. and Europe has focused on the mandated protection of data of specified types in regulated industries. Penalties for non-compliance to these mandates include high fines and prison terms for senior officers. This has spurred a renewed interest in data protection at the boardroom level and a need to ensure that compliance issues are being met at remote sites as well as centralized locations. This argues for the enterprise taking all steps possible to ensure the safety of backups performed at their remote locations. Consideration of the practices in this report should be part of that effort.

### *Critical Practices for*

---



# GST Research Report

---

## Remote Backup

### **Remote Backup**

The guidance provided here is meant to assist organizations in developing better data protection practices where remote backup processes are involved.

#### **Introduction**

Protecting each day's newly accumulated data in the enterprise is of great concern to management. When new computer transactions occur at remote branch or store locations, the challenges to capture and archive that information in a protected fashion are greater. Recently, this need to safeguard data so that it cannot be erased or altered has become even more critical because of legislated mandates for data protection processes by oversight bodies that issue stiff fines and prison sentences.

The failure of a backup operation can quickly reach catastrophic proportions. A common way this occurs is when in the *same day* that the backup operation fails there is a computer failure and the system goes down. In this case, earlier backup data must be accessed to initiate a Restore Operation to restore the computer to the state it was in when the most recent successful backup was achieved. The difficulty of locating and restoring the changes *since the last backup* becomes greater the longer the time interval since the last backup occurred. Each hour that the system remains down (downtime) can cost millions of dollars for organizations where critical applications are handled on-line in a real-time environment. When the only copy of the backup data from a remote backup has already been transported to the home office, recovery times can take even longer. For every organization, there is a point, beyond which it cannot survive if computer operations are not restored.

We now know that organizations that loose access to their computer applications and data for periods as short as a single week run the risk of going out of business within the next few years. This is particularly true when applications that cannot function without computer resources lost, such as Data Warehousing, Data Mining, Business Intelligence, Electronic Data Interchange (EDI), Group Computing and ERP applications like Manufacturing Requirements Planning (MRP), Supply Channel Management (SCM), Customer Relations Management (CRM)

The Gartner Group reports the following facts in connection with company disasters:

- Nearly 75% of all U.S. businesses have experienced an interruption.
- 20% of all small to medium businesses suffer a disaster every 5 years.
- 43% of all U.S. companies never re-open after an unexpected business interruption and 29% close within 3 years.
- 93% of companies with a significant data loss are out of business within 5 years.

A recent study by Contingency Planning Group shows that the financial impact of downtime is both well-documented and serious:

- Nearly half of all companies report each hour of downtime costs them at least \$50,000.



# GST Research Report

## Remote Backup

- One in four companies report the cost of downtime ranges from \$250,000 to a \$1million or more.

The data protection objective at remote facilities is that backup operations, recovery, archiving and disaster recovery measures are performed efficiently and correctly every time. Although this can be challenging, the consequences of not doing this can prove fatal for the enterprise.

The practices presented here aid in accomplishing this objective.

### 1. Let the restore process drive the backup.

“The most important question to ask when planning the backup process is *How do you plan to handle the recovery?*” reports Tim Kormos, Product Manager at [LXI Corporation](#), a maker of enterprise storage management software in Irving, TX. Kormos elaborates, “Recovery planning must always drive backup planning. A strong focus on the recovery process is even more important when the backup is remote, since the individual performing the backup and restore operations is often not proficient in IT technology. The recovery strategy defines the level of risk tolerance your company is willing to face.”

Kormos reports, “Failure to develop a recovery plan before the backup plan is comparable to buying all the materials you think you’ll need to build a house without first creating a blueprint. Chances are very great that something will be missing. Unlike building a house, in a critical recovery situation, if you don’t backup everything you need you can’t just run out and get the data you’re missing. A comprehensive recovery plan must define how the hardware is to be repaired, replaced or restarted, what steps must be taken to ensure that the most current version of the data is available, how the data will be restored, and who will be responsible for each task.”

Kormos continues, “To establish the risk your organization is willing to live with, three measures must be established:

- RTO - Recovery Time Objective: the amount of time your organization can be without the individual system or application; also called acceptable downtime.
- RPO - Recovery Point Objective: sets the amount of data that will be lost from the last backup.
- DPW - Data Protection Window: the amount of time you have to perform your daily backups.

A smaller RTO (downtime) leaves you with less available recovery time and this means you need to perform more comprehensive backups which lengthens your DPW. These combine to produce a minimal data loss (RPO). By setting clear targets for these three objectives, management can set the guidelines within which remote backups must function.”

### 2. Clear remote backup procedures.

Most remote backup operations involve one or more servers at the remote location that need to be backed up every night. Some remote operations completely backup all servers at a location on the weekend after closing, and backup the daily changes each day during the week. This latter approach results in shorter backups during the week, but adds to the complexity of restores, since multiple backup tapes are required to restore the remote server.



# GST Research Report

---

## Remote Backup

Tim Kormos of LXI emphasizes, "Careful training of the personnel handling remote backups goes hand-in-hand with well-crafted procedural documentation. Most remote backups are operated and managed by store personnel with little or no training in information technology (IT). Therefore, procedures associated with backing up and storing/transporting backup media at the remote store level must be simple, clearly written and tested thoroughly; then all personnel involved with backup processes must be carefully trained, since most backup failures can be traced back to operator error. Written procedures need to provide detailed instructions on how to contact support personnel for technical assistance, including what to do when the normal technical support people don't respond quickly. These procedures should be reviewed/tested at least annually, should be managed by the individual responsible for data protection, and should be stored in a safe and easily-accessed location, ready for immediate use should anything go wrong during a backup."

### 3. Use of an operator panel.

Most backup devices, including tape drives and optical drives, have some way of communicating status information to the operator. In a remote environment, the capability of the drive to communicate detailed status information is more critical. A good list of the types of information that operators can benefit from, is the data that GST provides on its LCD Operator Panel:

**Presence:** whether a tape cartridge is present or absent in the tape drive. This fact is not always visible by simply viewing the drive.

**Ready:** whether or not the tape drive is ready for operation.

**Clean Me:** the need for cleaning functions to be performed on the drive.

**Read:** shows when a read operation is taking place in the drive.

**Write:** shows when a write operation is taking place.

**Load:** shows when a tape cartridge is being loaded into the drive.

**Unload:** shows when a tape cartridge is being unloaded from the drive.

**Rewind:** shows when the tape cartridge is being rewound.

**Position:** shows when the tape cartridge is being positioned prior to reading.

**Remaining MB:** shows remaining megabytes of unused capacity on the tape, updated as data is written to the tape. Display is in uncompressed bytes. It can be used to determine when the tape has reached its capacity.

## Remote Backup

Display of the complete status of the backup drive and media is essential to provide inexperienced operators of backup and restore functions with an awareness of the critical performance and operational measures of the backup unit. This additional information can eliminate errors made by operators acting on incomplete information.

As examples of operator panels that provide a deeper level of information to the operator, pictures of two different GST LCD Operator Panels are shown below:

- AIT tape drive with LCD - [http://www.gstinc.com/images/int\\_ait\\_hires.jpg](http://www.gstinc.com/images/int_ait_hires.jpg)
- AIT tape drive with LCD up close - [http://www.gstinc.com/images/int\\_aitcloseup\\_hires.jpg](http://www.gstinc.com/images/int_aitcloseup_hires.jpg)

The more complete the status information is for the drive performing the backup, the more effective the operator will be in working with tech support personnel in the problem identification stage, as well as in getting the problem fixed and the backup completed.



GST AIT Drive with LCD

#### 4. Expanded capacity with dual drives.

Backup devices have a finite capacity for holding backup data. For tape drives this capacity has grown dramatically, to the point that the new super-drives in tape technology hold dramatically more data. The capacities below are native capacities and can be more than doubled when data compression is also used:

Drive	Native Capacity
SAIT-1	500 GB
AIT-3	100 GB
SDLT 600	300 GB
SDLT 320	160 GB
LTO-2	200 GB

For many remote locations, one of these higher-capacity drives will be more than sufficient to do a full-system backup each day. In some cases, even lower-capacity drives will be sufficient for backup operations. Eventually, the backup could require more capacity than exists with a single drive, even when compression is used to expand capacity. When additional capacity is required, there are several options:



## GST Research Report

---

### Remote Backup

1. Upgrade to a larger, and normally more expensive, tape drive.
2. Have the operator stay on premises until the first tape is full, to insert a second blank tape.
3. Add a second tape drive.

Dual drive configurations, like GST's AIT Dual Drive Tape Subsystem, can begin as a single AIT-1 drive with 91GB of capacity (assuming 2.6:1 compression) and grow to an AIT-3 drive with 260GB compressed. Any of the AIT drives (AIT-1, AIT-2, AIT-3) can be field-upgraded later to a dual-drive AIT tape subsystem when capacity needs to be doubled. This approach protects the investment in the first drive, and doubles the amount of unattended backup capacity available at the remote location. In most cases, the next-generation drive (say, LTO-2) can read the earlier generation (LTO-1) and even write in that format.



GST Dual LTO Tape Drive

#### 5. Mirrored backups with dual drives.

Mirroring the backup process by using dual drives can add additional insurance. Dual drives using Mirrored Backup Technology can produce identical sets of backup media simultaneously. One backup set is safeguarded remotely for rapid access in the event that a disaster recovery procedure needs to be initiated, thus ensuring the rapid deployment of DR activities. A second identical set of backup cartridges can be retained at the remote site to be immediately available for expediting the restore process.

Producing a duplicate set of backup media using a single-drive configuration requires a separate manual process to copy the backup set to create a duplicate set.

Besides eliminating a separate copy step, Mirrored Backup Technology eliminates the need to restart and repeat a save or restore process when a tape drive or media cartridge fails. GST calls this **Fault Tolerant Backup** and it takes two forms:

- **Drive Fault Tolerance** – If one drive fails during backup/restore, the second drive continues with the operation, ensuring its successful completion.
- **Media Fault Tolerance** – If one tape is bad, breaks or cannot be found for a restore or DR operation, a second set is readily available so that serious delays can be avoided.

GST's Mirrored Backup Technology provides added tape functions:

- **Off-Line Copy** – One set of backup cartridges can be copied to a second set, producing duplicate backup tapes. No server cycles are used.
- **Off-Line Verify** – Same as Off-Line Copy, except the data on the cartridge in one drive is compared and verified to be identical to the data on the cartridge in the second drive.
- **Cascade** – Permits switching control from one drive to another drive, once the first drive has completed backing up or restoring. Cascade doubles the backup's unattended save and restore capacity.

Mirrored Backup Technology provides an additional level of protection to mitigate against the growing array of threats that can bring a system down and the remote location along with it. When considering a mirrored backup solution, find out if you can start with one drive now, and expand to a dual-drive configuration later when it's needed while fully protecting the investment in the initial drive.



GST Mirrored AIT Tape Unit

### 6. Expanded capacity with autoloaders.

Just as a second drive can help to expand capacity, an autoloader can be even more effective in delivering additional capacity. That is because an autoloader is a single backup drive that has a magazine with up to 10 media cartridges. The automation part of the autoloader feeds each cartridge to the drive as it is needed.

Autoloaders are available for most advanced tape technologies, including AIT, Super AIT (SAIT), LTO and Super DLT (SDLT). Autoloaders provide unattended backup capacities ranging up to a Terabyte (2TB compressed). Autoloaders generally span the gap between single- and dual-drive backup units on one end and tape libraries on the other end, adding considerable granularity to an organization's array of backup units. As an example, with GST's 8-cartridge AIT-3 Autoloader, total unattended backup capacity exceeds that of a single AIT3 tape drive by 7 to 10 times. Most autoloaders have an LCD panel for advanced operator visibility over backup operations and the autoloader's automation robotics. A summary of the autoloaders that GST offers is below:

AutoDR™ Family - Workgroup Autoloaders				
Technology	Drives	Slots	Capacity <sup>1</sup>	Speed <sup>1</sup>
AIT3, AIT2, AIT1	1	8 - 10	700 GB - 2.1 TB	37 - 112 GB/hr
LTO2, LTO1	1	8 - 10	1.6 - 4 TB	108 - 252 GB/hr
SDLT600, SDLT320	1	8	2.6 - 4.8 TB	115 - 260 GB/hr
SAIT1	1	10	13 TB	280 GB/hr
SLR100	1	8	800 GB	36 GB/hr

<sup>1</sup> Assumes Compression



GST SAIT Autoloader

### 7. Backup over the Internet.

Another way to do backups at remote locations is by using the Internet. This backup accomplishes the same objective, but with one major difference. The backup data on the remote server is not sent to a tape drive or other media attached to the computer being backed up. Instead, specialized software transmits the backup data over the Internet, or even regular telephone lines or another network connection, to a specialized backup server at the central IT site or to a safe remote site where catastrophic events that could destroy archived data is highly unlikely. This backup process can be executed after the remote location closes for normal business, or it can be performed at any time during the day.

This process can be fully automated, without the need for anyone at the remote location to start up the backup process. In this case, the backup hardware that is needed at the remote location is a high-speed connection to the Internet.

### 8. Take advantage of tape management systems.

We interviewed Tim Kormos of LXI on this topic and this is what he had to say, “By using tape management systems that track the utilization of every unit of backup media, the chance that a tape will be accidentally overwritten is virtually eliminated. Of considerable importance, especially when data is needed for recovery, is the ability to locate the required data quickly and to execute the restore with the correct tapes. A tape management system will also ensure that only scratch tapes are used for backups, so vital media with important backup data is not overwritten.”

Kormos continued, “Keeping track of media requires two very specific practices. First, each tape should have a unique *external* identifier. The identifier can be any combination of alphanumeric characters. Typically, this identifier is up to six characters long. A second practice is that all externally labeled



# GST Research Report

---

## Remote Backup

(including bar coded) media should be initialized with an *internal* label to match the external label. This is most commonly referred to as the *standard label format*. It's important to note that tape management systems for open systems servers do not necessarily enforce the requirement that the internal label must match the external label, so procedures should be established that require a verification step to ensure this is done."

### 9. Importance of reliability.

The reliability of the backup unit is critical when the unit is functioning in a remote location, far from the organization's IT resources and replacement parts. Reliability measures how well a device or media cartridge functions over time in demanding operational conditions. There are a number of measures related to reliability that should be considered when selecting a backup device for use in remote locations:

**MTBF** – Mean Time Between Failures, or Mean Time Between Faults, measures the average time expressed in hours that a component is expected to work without failure. It is most affected by the quality of the unit and the environment in which it is operated. MTBF ratings are calculated by dividing the total number of failures into the total number of operating hours observed. Also, see:

<http://www.webopedia.com/term/m/mtbf.html>.

**MSBF** – Mean Swaps Between Failures measures the number of cartridge swaps in an autoloader or tape library between failures. For more information:

[http://whatis.techtarget.com/definition/0,,sid9\\_gci821041,00.html](http://whatis.techtarget.com/definition/0,,sid9_gci821041,00.html).

**Duty Cycle** – This is the assumed amount of time the device is ON and running and is always stated for an MTBF value. The best duty cycle for comparing MTBFs and MSBFs is 100%, meaning the device is ON continuously.

**Head Life** – This is the number of hours of running time for which the read-write heads in the drive are engineered to last.

Additional reliability measures that apply to media itself include:

**Media Uses** – This is the number of end-to-end passes that the media/cartridge is designed to provide before a failure occurs.

**Archival Life** – This is the number of years that the media can be safely stored, assuming the manufacturer's specifications for media storage are followed.



# GST Research Report

## Remote Backup

Below is a table showing the data for these important reliability measures for the leading types of tape drives available today.

Specification	AIT-3	AIT-2	VXA-2	SLR100	AIT-1
MTBF (Hours)	400,000	300,000	300,000	300,000	300,000
Duty Cycle	100%	100%	12%	100%	100%
Head Life (Hours)	50,000	50,000	N/A	10,000	50,000
Media Uses (end-to-end passes)	30,000	30,000	N/A	N/A	30,000
Media Archival Life	30 years	30 years	30 years	20 years	30 years

Specification	SAIT-1	SDLT 600	LTO-2	SDLT 320	LTO-1
MTBF (Hours)	500,000	250,000	250,000	250,000	250,000
Duty Cycle	100%	100%	100%	100%	100%
Head Life (Hours)	50,000	30,000	N/A	30,000	60,000
Media Uses (end-to-end passes)	30,000	17,850	5,000	17,850	5,000
Media Archival Life	30 years	30 years	30 years	30 years	30 years

### 10. Importance of Durability.

**Durability.** The way that drives are engineered can have a big effect on their overall durability. Why is durability important? Most remote locations pay little continuous attention to where the backup device is located or the physical environment in which it resides. Resistance to vibration and shock, moisture, heat and dust all go into the durability of a drive. GST uses LTO tape drives manufactured by Certance to take advantage of built-in durability features to endure shock and vibration and to protect tape cartridges from airborne particulates.

Ryan Malone, Senior Product Marketing Manager at [Certance](#) notes, “SmartVerify and MediaShield address this issue in our LTO drives, maximizing durability of the drive and doubling media life. SmartVerify uses technology from the cruise missile industry to ensure drives read and write correctly even under continuously high vibration and extreme shock. MediaShield keeps heat and dust separate from the media and uses low-friction tape guides to reduce wear on the media itself. The result is a high-durability solution that offers nearly twice the media life of alternatives. “

### 11. Importance of Repair Time.

Typically, the time for a service technician to get to a remote site to service a failing backup unit is much greater than when the unit is located at the central IT location. Functions performed by the technician include diagnosis and repair or replacement of the backup drive or replacement of damaged media. Two important measures that affect the ability of an organization to service a failing unit are:

**Response Time** – This is the time it takes for either a repair technician to reach the premises of a device needing service, or for a technical support service linked via internet or telephone to respond to a call for help from a user.



# GST Research Report

---

## Remote Backup

**MTTR** – Mean Time To Repair measures the time it takes to repair or replace a unit once the problem has been diagnosed. More information about MTTR can be found at: <http://www.mttr.net/>.

Both of these measures should be reduced as much as possible to ensure rapid technical response and support for backup devices at remote locations. The difference between getting a remote location's backup or restore going again in one hour versus three hours can have a significant impact on that location's operation.

### 12. Get data off your premises quickly.

Hand-in-hand with efficient operation of backup and recovery processes, is the need for off-site protection of data. The best strategy for backup data is to transport it to a safe and remote location as quickly as possible. The location can be a storage vault providing secure storage, or a Disaster Recovery site where computers are available to replace your remote computer operation should the remote site's server go down or be destroyed in a disaster.

A key element in transferring backup data to a DR site is to have it removed quickly from the computer site, since as long as it sits at the site, the site's backup data is not safe from an on-site disaster. Having the emergency number readily available for the transport service that picks up the backup media is important. Another key practice is conducting rehearsals of the procedures for using backup media stored at the DR site to ensure readiness in case a DR operation is ever needed. These disaster rehearsals are critical for an effective data protection strategy and can be planned and executed with the assistance of the DR service organization used.

### 13. Key technical concerns.

A variety of technical concepts should be considered when planning for remote backup:

**Hot-swap backup drives.** This capability allows backup drives to be removed and replaced in backup devices without taking the entire server down. This is of obvious benefit to the remote site, allowing the drive to be changed while employees are using the server.

**Redundancy of backup drives.** When an additional backup unit can be stored at a critical remote location, the backup drive held in reserve will ensure that backups can be made even if the backup device installed is inoperable.

**Alternate sources of power.** Whenever there is the possibility of the server or backup device tapping into an alternate source of power, then there is one less change for the backup to be thwarted. Alternate sources of power are best planned for at the time the server is installed, but can be added afterwards.

**Choosing a safe location.** Remote location management should be aware of the importance of storing the backup unit in a safe location. Staying away from overhead sprinklers and air vents that could eject dust are two of many issues to consider when selecting the location for the server and remote backup unit.



# GST Research Report

---

## Remote Backup

**Media handling.** Even when a good backup has been prepared onto media, there is the danger of mishandling the media and jeopardizing the validity of the stored data. Good practices for handling, storing and transporting media are usually available from the media manufacturers and should be identified and followed carefully.

**Encryption of backup data.** If backup data is lost or stolen, there may be confidential data that should be kept private. Encryption devices are available to ensure that backup data is encrypted and can only be read by the organization making the backups. One example of such a device:

<http://www.gstinc.com/products/encryption/index.html> .

### 14. Give the person backing up the system proper authority.

Whoever is in charge of backups and restore operations within your organization, holds the institution's lifeblood in their hands. Make sure they have enough authority to make necessary decisions on the spot. There should be a clear channel of communication from the person responsible for data protection at the remote site to their superior and to the CIO and Risk Manager within the organization. This is now doubly important with new compliance regulations like the Sarbanes-Oxley Act (see Compliance issues below) that mandates the way data must be backed up, stored and protected.

### 15. Compliance issues.

U.S. federal and state regulations requiring specific data protection measures are coming into force this year and will only become more stringent over time. These regulations apply as much to the protection of data in remote, outlying sites, as to central IT locations where policy is made. Tom Huntington, VP of Technical Services at [Help/Systems](#), a provider of automated operations software located in Minnetonka, MN, says, "Obviously the Sarbanes-Oxley Act (SOX) is a hot topic for many IT shops and the implementation date of November 2004 is approaching rapidly. Many customers are calling and asking if our line of backup software is compliant? The answer is automated backup software can *help* you become compliant, but you still need to set software and procedures up correctly. For instance, if you continue to execute your backups using your old control language program scripts, our backup software won't provide that much help."

Huntington continues, "Your old backup methods and practices might get the job done prior to SOX, but with SOX coming, you need to make sure your procedural documentation is current, since SOX mandates organizations to show and demonstrate that they have documentation, policy and procedures in place for backups. If you have to update this continuously, it can cost you time and money. Having automation in this area can be cost justifiable to upper management."

Clearly, software won't cover the new compliance regulations alone. Carefully developed and rigorously documented procedures that ensure backup data is shielded from alteration and removal are necessary. An important new development addressing the unalterability of backup media is WORM (Write Once-Read Many) technology. WORM tape drives, from Sony Electronics, ensure that once data is written to tape it cannot be erased or altered in any way. Sony-built AIT2 and AIT3 drives that GST provides in its AIT tape solutions provide this new WORM technology; AIT1 drives do not include WORM technology. "WORM is also available in the SDLT tape technology and is expected to be announced by 4Q 2004 from the LTO Consortium that produces LTO-1 and LTO-2 now and is developing LTO-3," reports Ryan Malone of Certance.



## GST Research Report

---

### Remote Backup

Some of the U.S. compliance regulations with mandates that WORM addresses include the Sarbanes-Oxley Act, the Healthcare Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act, the Patriot Act, and the Federal Drug Administration's 21 CFR Part 11 for the pharmaceutical industry.

Compliance is an issue that continues to evolve as new legislation is produced and deadlines are reached. It requires continuous monitoring by someone in the organization responsible for this function, to assure that remote sites are brought into compliance and remain there.

-END-



# GST Research Report

---

## Remote Backup

### 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)

### Related GST Research Reports

Click here for a complete list of GST Research Reports on data protection.

<http://www.gstinc.com/white/index.html>

### About the authorship of this paper

This GST Research Report was prepared by GST's Research & Engineering Group under the leadership of David Breisacher, CEO/Chairman at GST. David is the founder of several successful companies, including GST and BCC Technologies, a manufacturer of eServer disk, tape and memory storage devices. A visionary for the storage industry since the early 90's, David lends his market insight and predictions for the IBM midrange storage marketplace to the research conducted at GST. His experience in sensing shifts in technology and industry directions has made it possible for him to organize and structure successful companies to rapidly meet the evolving needs of storage users.

### About GST, Inc.

GST, Inc. (<http://www.gstinc.com>) engineers, manufactures, markets and sells a line of innovative storage products to meet the need for high-performance, continuous reliability and cost-effective data storage. These products include tape solutions available today, and will include storage-related services, software and disk subsystems in the future. A comprehensive array of tape solutions range from single and dual tape subsystems, autoloaders, midrange tape libraries, to modular enterprise-wide tape libraries, with focus on improved backup and disaster recovery solutions. Modular design enables field upgrades, scalability, investment protection for existing GST tape solutions, and lower life-cycle costs. GST's product development is guided by several advisory boards to closely track market needs and fully utilize the latest engineering developments in product design. Complete information about products, support and company background can be found at the company's Website.

### 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. AS/400, iSeries, IBM, UNIX, Linux and Windows are the property of their respective owners.