



Backup You Can TrustSM

BRU's Support of Regulatory Governance

Preface and Acknowledgements

The information contained in this white paper is offered to:

- Share perspectives about regulatory governance and how to address it in the first half, and
- Detail the key characteristics of BRUTM technology that provide the accurate backing up, restorability and overall availability of data required in regulation mandates

This is the sole spirit of this document, and no legal representation concerning the Acts referenced is intended, nor should be inferred.

While this paper samples regulations promulgated through U.S. legislation, similar governance is being instituted around the globe and mirrors, to a very large extent, the intent of the U.S. regulations.

The information contained in this paper is both TOLIS developed and supplied by outside sources that track and provide regulatory compliance expertise.

TOLIS Group gratefully acknowledges Dorian Cougias, CEO of Network Frontiers and author of The Backup Book (Schaser-Vartan Books) for his contributions to the development of this paper.

Regulatory Governance - Why Should I Care and/or Read This Paper?

If your organization is privately held, perhaps you don't have to care about regulatory governance - at least not yet. If your organization is a public corporation or a not-for-profit organization, there are two (2) reasons why you should be interested to read this paper:

- You have already been audited, failed to comply with a regulation or regulations, and are looking to make sure you do not experience a repeat performance.
- You don't know if your organization will pass a compliance audit and you need to accumulate knowledge to make informed business decisions to assure compliance.

In either case, the following information shares valuable regulatory insights and is presented in conversational English rather than legalese.

The Pervasiveness of Regulatory Compliance

There are over 9,000 regulations worldwide that regulate business practices across a breadth of industry segments.

Examples of the major regulatory policy instituted by the U.S. Government include: the Health Portability and Accountability Act (HIPAA, healthcare), the Security and Exchange 17a-4 (financial services), the Gramm-Leach-Bliley Act (GLBA, consumer privacy), the Sarbanes-Oxley Act (Sarbox, corporate accountability), ESIGN act (electronic business records), DOD 505.2 (government) and the USFDA 21 CFR (life sciences) Acts to identify a few.

Current regulations are evolving, and new ones are being developed virtually on a daily basis.

The common thread throughout these and other Acts worldwide is the mandated treatment of an organization's information including: how long it must be kept, its availability, auditability, integrity, accuracy, privacy and security.

While the benefit from some of the governance is evident and warranted (and perhaps overdue), it is clear some legislation touches the far side of a reactive pendulum swing. Rest assured, more Acts will follow - both good and bad.

Distilling Regulatory Compliance

Regulatory compliance can be simplified into the following realities:

- Multiple regulations are going to impact an organization's storage decisions and policies
- Organizations will have to retain and protect more information, and for longer periods than originally thought in formats such as: e-mail, pdf, spreadsheets, word processing documents, audio & video clips, etc.
- Compliance is significantly more involved than merely implementing hardware and software solutions
- The regulators are doing this because they want the data availability when they want it

Incredibly, while working your way through the compliance morass, you can do more with less to be in compliance if you plan smart and plan with a long-term focus.

Although not all mandates apply to every segment, it is imperative to remain within compliance. At this juncture, public and not-for-profit organizations are governance targets. Adherence to the majority of dictums by understanding the cross-Act commonalities will position an organization well when audited.

Compliance Mindset

By approaching regulatory compliance as a "process" instead of a "project," a level of sanity can be maintained as well as long-term focus. This is important and necessary work because the cost of non-compliance can far exceed the time, effort, and cost of compliance.

An organization approaches compliance as a process when it takes a "best practices" approach- via implementing the policies and procedures that pass the litmus test of: *"Did your organization act reasonably given the circumstances?"* An affirmative answer positions an organization well against the scrutiny of an audit.

When compliance is approached from a project perspective, it becomes a never- ending, very costly quest that results in boundaries too limiting in scope.

Identifying Governance Pressure Points

Given the myriad of regulations, one would think that all data is impacted. Not so, and not yet. That said, the guidelines are not set in stone and are a constantly moving target. A good rule of thumb to identify an organization's regulatory data is:

"Information that drives your organization, or is a source of competitive advantage or differentiation, is more than likely to be targeted as regulatory data"

Remember also, governance is not just about data, it is also about the policies and processes that manage the data. Stated another way:

"Any procedures or plans that secure and preserve your data will more than likely fall under regulatory compliance now or in the future"

Working Toward Compliance

Software application developers have recognized the market opportunity afforded by government mandates because they require, in some cases, a profound shift in the way organizations must operate. Therefore, dozens of applications have been developed to support regulatory compliance. As may be needed, senior management now has the necessary tools available to them to manage the policies and processes that will bring their organizations into lock step with the regulations. But process is only part of compliance - execution is equally important.

Compliance Has Two Faces

It is easy for organizations to unknowingly take a carpe diem approach when implementing regulatory-support applications by focusing their attention on the visible processes and policies consistent with compliance. Without an information support infrastructure, the best of plans will fall short of providing adequate protection for the organization.

Information regulated under the Acts can be dynamic, and ever changing (business decision information), or static such as a customer stock equity purchase transaction. In either case, protection is paramount. The strategies, policies, or published information based on dynamic data may be audited down the road. Without an audit trail, organizations place themselves at risk, and that risk now even extends directly to management levels such as CFOs, CEOs and Directors.

While senior management typically take a hands-on role in choosing which regulatory-support application to purchase because of the high visibility of governance (remembering executive liability now), the decisions regarding how to actually protect the data for future access is typically deferred to the IT staff.

Given the movement away from physical hardcopy toward digitally stored information, the decision about which software tool or tools used to achieve compliance is a most important one.

BRU's Support of Regulatory Governance

The remainder of this paper specifically addresses BRU technology, and its ability to protect digital information by either copying or permanently offloading it from a primary computer system that supports an organization onto intermediary and/or non-volatile archive media. BRU Server™ is the

solution specifically addressed in the following sections.

"99 percent of IT sites in North America don't know how much of their data is actually recoverable."

This statement should be of great concern within any organization, but especially to those that fall under regulatory governance. Aside from compliance to government mandate, it is prudent to protect all information - arguably an organization's most critical asset - whether or not subject to governance.

Organizations must be able to enjoy an exceptionally high confidence level that their backup software can successfully retrieve information. An auditor expects it, and so should the organization. While no software can deliver 100% data recoverability because of potential physical damage to the archive media, BRU technology delivers unprecedented data availability and recoverability when viewed against all other backup tools.

Difference Between UNIX® and Windows®-based Backup Tools

UNIX can be characterized as an "intelligent" operating system. As such, it inherently supplies conformance to select regulatory data compliance mandates at the operating system level. BRU technology provides native UNIX system support and leverages the characteristics within UNIX that automatically provide compliance to governance. The benefit is greater simplicity and streamlining at the backup system software level.

Windows on the other hand does not provide the same level of native data management provided in UNIX. Therefore, Windows-based data protection tools must incorporate the necessary support within themselves. This results in increased bulkiness and overhead at the backup software level.

Is the Data Recoverable?

An organization must be able to answer this question "yes" - with certainty. Data recovery is not a religion, and "beliefs" hold no value when an audit occurs.

The focus of BRU's early development was the ability to restore data. This is a subtle yet profound difference compared to other backup tools. This unique design philosophy structured the BRU data format and the incorporated checks and balances needed to assure data recoverability. In effect, the BRU restore operation defined how the BRU backup operation works.

BRU's reporting verbosity is deep, and the level of reporting is user selectable. Should an error occur during the backup, BRU reports the occurrence with specificity. This is in contrast to some backup tools that will actually write data streams to an inoperative device without reporting an error. Without responsible reporting, system administrators will never know the status of the backup, and if it completed - successfully or otherwise.

Most backup software tools are based on the traditional data formats such as tar, cpio, and MTF (Maynard, or subsequently "Microsoft" Tape Format). These formats are flawed in their ability to assure the data transferred from Point A to Point B actually made it. A simple test can be used to prove the assertion, located at: <http://www.tolisgroup.com/pdf/ProvingTheBRUAdvantage.pdf>

The successful completion of a backup is only the first-step to information recoverability. The information that was archived must be proven to be accurate.

Garbage In/Garbage Out

Each backup holds the recoverability of information hostage. If the backup is not accurate, then accurate recoverability becomes impossible.

Each BRU backup can be 100% verified for accuracy. BRU divides the backup data stream into "buffer blocks," and calculates checksums on both the header and actual data. It is these checksummed buffer blocks that serve as the basis for BRU's leadership backup accuracy verification and data recoverability. TOLIS' white paper titled: "The BRU Advantage," detailing BRU's leadership logical approach to data protection is available at:

<http://www.tolisgroup.com/pdf/TheBRUAdvantage2003.pdf>

Following the backup it is important to verify its accuracy (garbage in/garbage out). Virtually all backup tools implement one of the following verification strategies:

- **Bit-level Comparison:** Doing a bit-level compare requires the system or network to be quiesced so the contents of the archive can be compared to the system disk(s). Should a user simply read a file during the bit-compare, the "atime" characteristic of the file is changed and an error will be logged. The administrator must then determine the cause of the error. In the real world, these errors are almost always ignored and the successful recoverability of information is placed at risk. If a backup takes 1 hour, an additional 1-hour is needed to conduct the bit-level compare. (BRU does provide bit-level compare as an alternate verification choice)
- **Metadata Checksums:** Some tools checksum only the metadata, and not the actual data. It has been seen where the metadata has been successfully backed-up and no actual data was included. The backup was proofed, yet was useless.
- **Trial Restores:** To validate a backup, some tools will recover several files. If successful, the entire backup is considered to be good. This strategy is flawed, and the failure to recover other data in the backup comes as a surprise.
- **Tape Drive ECC:** Some backup tools rely on the ECC (Error Correction Code) capabilities of the archive device to verify the backup. This logic is severely flawed because the ECC cannot recognize good or bad data coming into its buffer. Tape device ECC can only verify that what was received into its buffer was written onto the tape. TOLIS' white paper titled: "Reliable Verification vs. Tape Drive Read After Write and Hardware ECC," located at: http://www.tolisgroup.com/Reliable_Verification.pdf clearly details the pitfalls of reliance on tape device ECC to verify the backup.

In contrast to all other backup tools, BRU's structure negates the need to access the disk or disk farms to fully verify the backup. All of the information needed (all-inclusive checksums [metadata/actual data]) to proof a backup resides on the archive media.

As a result, the verification process can be done in an out-of-band process that allows the primary system to be available to users immediately following the backup. *This process reduces the backup window of a fully verified backup by at least 50%, compared to other tools.* BRU backups can even be verified on a different system and operating system (cross platform compatibility is covered later).

Using BRU technology, information archives can be re-verified/re-validated whenever required by regulations - even 10 or 20 years from the date of creation (dependent upon media life expectations). The robust verification procedures built into BRU provide system administrators with an uncommon peace-of-mind that the information is safely protected and is retrievable.

By exacting design, BRU technology pays attention to filesystems, files, permissions, archive devices and their media to be the most reliable backup software tool available.

All Restores Are Not Created Equal

An accurate backup does not insure that information can be accurately recovered when needed!

Restoring an accurate, unadulterated backup is not a challenge for modern backup software. Regulatory governance mandates how long information must remain available, typically longer than an organization would normally retain it. Because bits can become physically altered (scratched) or electronically altered (magnetic degradation) following a good backup, the immediate and long-term recovery of data does become a challenge.

In contrast to all other tools, BRU does not abort the recovery process when altered information has been detected. When restores are aborted, any remaining information that has not been recovered if/when corrupted or altered data is encountered becomes irretrievably lost. When BRU technology experiences altered/corrupt data during a restore, it makes multiple attempts to read the bad area. If it cannot, BRU reports the error location with specificity, advances the media to the next good BRU header block and continues the restore. Under similar conditions, no other backup software is capable of returning more data than BRU technology.

Uncommon Data Protection Detail

Data backup and restore is the visible tip of the data protection iceberg; so much more happens below BRU's "waterline."

In addition to the checks and balances built into BRU logical data format to assure reliability, BRU incorporates additional functionality to augment data availability.

The BRU Server catalogs are written to the target device media (disk stage or tape) in addition to the backup system HDD (hard disk drive) to provide a heightened level of availability to the data. Should the backup system HDD fail; the catalogs that are the roadmaps to your archived information will be lost. Using other backup tools, the catalogs must be manually re-created - a very time consuming effort fraught with opportunity for human error.

When using BRU Server, an "automatic scan" of the backup media can be initiated and BRU rebuilds the catalogs and places them onto the backup system HDD without further human intervention.

Agnostic Device Support

BRU data protection software is not tied to the target device, which can be a very limiting characteristic.

BRU technology provides native support of target devices and does not require special device drivers, regardless of the technology: Magneto-Optical, tape, etc. This means within an archive technology family (i.e. AIT1 to AIT2 to AIT3 to downstream AIT-4 and AIT-5 iterations), current and future releases of BRU will continue to write archives that can be read today or tomorrow.

The benefit of this capability is today's devices within a technology family need not be kept and maintained in order to read the archives down the road.

If an organization makes a wholesale switch to another archival technology or format at some point, the BRU archives can be read back into the existing system and redirected to new archival devices without the need to update/replace BRU.

Built-In Information Security

BRU's data format serves as an additional hurdle to help gate access to information from unauthorized prying eyes.

Regulatory language defines the security levels of specific classes of information that must be maintained.

Data encryption is one approach backup software tools implement to protect information. The information is encrypted in transit from the system to the archive device during a backup and visa versa during a restore. Should someone hack into an encrypted data stream flow - the data will be unintelligible and secure. During network data transmission, TOLIS' BRU Server uses powerful 256-bit AES (Advanced Encryption Standard) in conjunction with the Diffie-Hellman "key exchange protocol" to assure the safe and secure transmission of data across the network. The U.S. Government, except for its "E1" exclusion list, has authorized TOLIS' encryption for export to all nations.

Some backup software tools write the encrypted information streams directly onto the media. While the information is secure, operationally this approach has proven to be a dangerous strategy. While the encrypted information on the media protects against unauthorized access, it poses significant problems for those authorized to access it - most notably the loss of a password or key, rendering the information permanently irretrievable. Organizations can be in regulatory compliance whether or not the data is encrypted on the media.

BRU Server de-encrypts the information stream prior to recording on the archive media and lays the data on the media in the BRU format. A BRU archive cannot be read with traditional tools. This adds a level of complexity to protect the confidentiality of data. In order for unauthorized eyes to access the data, a BRU backup system environment must be created in addition to access to the passwords.

Within organizations that need access to information by multiple, authorized persons, BRU technology for larger organizations allows administrators to define the levels of security and information access points they wish to achieve or allow.

As mentioned, the U.S. Government has identified the classes of information that cannot be altered once archived. BRU supports native support of all WORM (Write Once - Read Many) technologies such as Magneto Optical (MO) and Sony's WORM AIT-2 and AIT-3 tape technology to create the immutable information archives now required by law.

Note, that while Write Once technology does support the regulations, its use is not mandatory. Acceptable policies and processes that assure captured data is not altered, used in conjunction with normal target devices that can write and re-write, are acceptable:

"The intrinsic control codes used by these systems cannot be turned off at any level. The systems must physically and logically protect the actual record itself and explicitly does not approve the systems that protect only at the application level."

The Disk Or Tape Backup Conundrum

WORM (Write Once, Read Many) technology is NOT required to comply - so why don't I just back up my data onto additional hard disks?

You can, and still remain in compliance. Whether or not this is a good strategy is an important business decision that must be carefully weighed. Factors such as expected data volume growth comes into play. As related in a subsequent section of this paper, some data must now be kept for more than 25 years. Since disk becomes an inversely effective strategy as the volume of data grows significantly, it may not be a viable component of a needed long-term compliance process previously addressed. There are many additional considerations such as geographically separating the archived information that becomes more difficult when using disk. The placement of regulatory covered data onto tape will be a component of regulatory compliance in most organizations.

BRU Technology supports D2T (Disk-to-Tape), D2D (Disk-to-Disk), and D2D2T (Disk-to-Disk-to-Tape) data protection strategies. A significant characteristic of BRU's D2D capability is the accuracy of transferring data from disk-to-disk is fully verified with the same robust precision employed when writing to tape.

Consistency In a World Of Change

The future cannot be predicted, yet BRU's architecture and linear and cross-platform compatibility delivers the consistency needed to assure the long-term protection of data.

Regulatory governance defines how long information must be kept. While simple in concept, execution becomes a challenge because of the frequent turns in technology. Technology advancements are a good thing, but today's hot flash soon becomes tomorrow's left behind "dust collector." The rapid pace of technology change places a strain on an organization's ability to retain levels of consistency and normalcy relative to accessing data. How long?

"The minimum length of time an organization must retain records varies by industry and spans, for example, from 1 year to retain hiring documents (corporate environment) to more than 25 years for information such as: plant ledgers (public utilities), pediatric records (HIPAA), transactions (SEC 17a-4)\and U.S. Government payroll records."

BRU was "born" in 1985 in response to a catastrophic loss of corporate data. Now, 18+ years later, the venerable BRU 17.0 kernel is the cornerstone of BRU Server, TOLIS' highly scalable data protection solution that supports regulatory governance across organizations of all sizes.

Since BRU's inception, the lineage of revisions represents evolution, and not revolution. Current and future BRU technology can, and will, read BRU archives written yesterday, last month, or even under BRU 6.1 released in 1987. In a backup tool world fraught with intra-application version incompatibility, this extraordinary level of BRU compatibility serves as a testament to the understanding and commitment to protect data the BRU heritage delivers.

In concert with BRU's compatibility across versions, cross-platform compatibility also exists. This means BRU archives can be read on any BRU-supported platform. Archives written on an HP-UX system can be read on an AIX system - on a Linux system - or on a Mac OS X system. One constant in computing, as organizations adopt new technology, is BRU's ability to return critical information back to them, supported from a variety of perspectives.

Architecturally, the data transport layer is transparent to BRU. BRU supports SAN and LAN environments, and provides flawless support whether the interface is SCSI, iSCSI, Fibre-Channel, Gigabit Ethernet, or even wireless LAN. BRU also provides native support of archive devices without the need to purchase special drivers, ranging from a multitude of standalone devices such as removable disk technology, disk-files, MO, and tape drives to the largest of tape libraries.

The scope of BRU's data protection coverage is industry leading, and there are no associated hidden costs to protect an organization's legislation-protected information.

Summary

Organizations that fall under the existing and emerging acts of legislation that mandate the treatment of information have no choice but to comply.

There are software application choices that manage the highly visible aspects of compliance, those that occur at a higher business operation level. Lesser focus is placed on the back-end support of compliance - namely the ability to recover information whenever needed to support a business decision or an auditor's request.

BRU is proven data backup and recovery technology that provides users with the peace-of-mind knowing their information is safely protected. BRU is a compelling solution to protect government-regulated information: delivering a breadth of functionality unique in the backup software market. BRU is cost-effective and delivers uncommon software investment protection.

Organizations may feel hostage to the legislated Acts, but BRU will not hold organizations hostage to their information. BRU delivers Backup You Can TrustSM.