White Paper

Regulatory Compliance and Operational Readiness: Complementary, but Never Synonymous

By Jason Buffington, Senior Analyst; and Monya Keane, Research Analyst

May 2013

This ESG White Paper was commissioned by Iron Mountain and is distributed under license from ESG.

© 2013 by The Enterprise Strategy Group, Inc. All Rights Reserved.

Contents

All trademark names are property of their respective companies. Information contained in this publication has been obtained by sources The Enterprise Strategy Group (ESG) considers to be reliable but is not warranted by ESG. This publication may contain opinions of ESG, which are subject to change from time to time. This publication is copyrighted by The Enterprise Strategy Group, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of The Enterprise Strategy Group, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact ESG Client Relations at 508.482.0188.

© 2013 by The Enterprise Strategy Group, Inc. All Rights Reserved.

Introduction

Recovering from a disaster or outage is a frightening prospect to ponder. Things get even scarier when you remember that disaster recovery is just the beginning of what you need to think about and act on—especially if you are responsible for IT at an organization in a regulated industry. Without doubt, you can count on these realities:

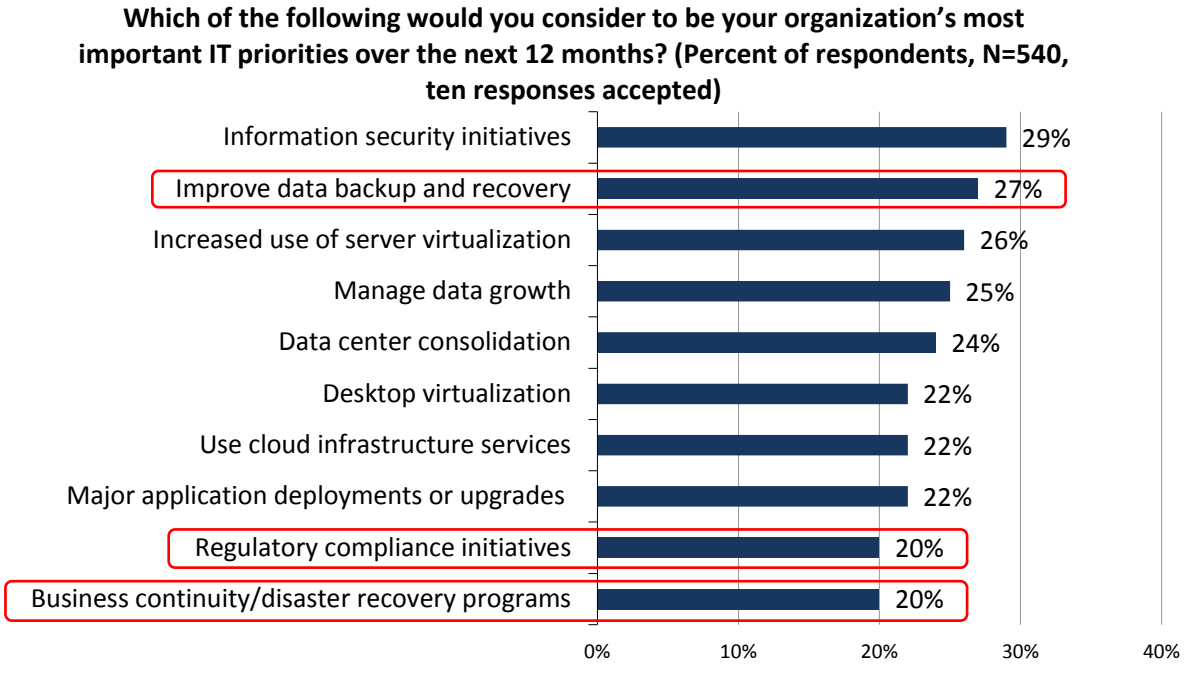
- Compliance is becoming ever-more rigorous and laborious.
- Mandates, rules, and regulations continue to proliferate in the U.S. and worldwide. One major multinational law firm that specializes in regulatory and government affairs has published an overview of *just* the data protection laws and regulations in effect as of March 2012 across 58 countries. The summary-level document spans 274 pages.[1]
- Even a "small" business disruption will likely have a big negative effect if you are ill-prepared to recover from it.

This paper discusses the differences between regulatory compliance (passing an audit) and operational readiness (being able to recover an IT environment). It summarizes a few of the key regulations germane to several highly regulated industries. Near the end of the paper, you'll find a section that evaluates a relevant Iron Mountain offering, the Iron Mountain Archival Tape Management solution, including an assessment of its capabilities in respect to the interrelated yet distinct topics of regulatory compliance and operational readiness.

Recent Research Findings

New ESG research on organizations' IT spending intentions this year has revealed a few *unsurprising* findings (see Figure 1). Namely, improving data backup and recovery, business continuity/disaster recovery programs, and initiatives to help the organization comply with regulations were identified by respondents as some of their most important IT priorities, placing them in the top-ten responses cited.[2]

Figure 1. Top-ten IT Spending Priorities for 2013



Source: Enterprise Strategy Group, 2013.

[1] Source: DLA Piper, *Data Protection Laws of the World*, March 2012.

[2] Source: ESG Research Report, *2013 IT Spending Intentions Survey*, January 2013. Regulatory compliance initiatives and business continuity/disaster recovery programs were tied at 20% with business intelligence/data analytics initiatives, improve collaboration capabilities, and deploying applications on or for new mobile devices.

© 2013 by The Enterprise Strategy Group, Inc. All Rights Reserved.

Why are the findings unsurprising? Those same three responses have made an appearance on ESG's annual IT spending intentions survey for several years, and their continued presence on the list of top-ten most important IT priorities reflects the fact that decision makers remain acutely aware of how important information is to their business. Data is the lifeblood of most modern organizations. It must be protected, preserved, and archived properly for efficient retrievability—perhaps to comply with internal policy, or perhaps under penalty of law.

In a similar vein, ESG research delving more deeply into spending related specifically to data protection showed that two of the most commonly cited challenges pertaining specifically to data protection involved:[3]

- Improving disaster recovery capabilities
- Meeting compliance requirements

Those findings are another indication that regulatory compliance is on the minds of people in charge of data center operations who are wondering whether their jobs will be on the line if an audit occurs and the data protection/recovery strategy is found wanting. Making the situation more challenging is the fact that regulations touching on data protection often use complex, convoluted language to dictate a result while shedding little light on how to achieve it.

Regulatory Compliance vs. Operational Readiness

Just because an organization *can* back up and restore data doesn't mean it *will* pass compliance audits that scrutinize backup and recovery. Nor does it mean the organization will be able to locate specific data when it is needed.

Compliance Capability

Depending on the regulation, true compliance might require that certain archival data be kept for a certain length of time (no more, no less). And in some cases, unless backups are being retained in accordance with *a particular sentence* in a particular regulation, the organization will not be compliant.

For example, the sixth sentence in section 164.310(a)(2)(i) of the Health Insurance Portability and Accountability Act (HIPAA) describes a particular type of facility-access contingency plan that must be in place to ensure restoration of lost data. ("The Covered Entity will need to establish a plan in advance with ITS to provide alternative computing resources to access ePHI as part of the Covered Entity's §164.308 (a)(7)(ii)(C) Emergency Mode Operations Plan.")

Readiness Capability

Conversely, it is possible for an organization to set up a data protection and recovery scheme that is capable of passing an audit but incapable of ensuring operational continuity should a disaster occur. Such an organization might have proven to auditors' satisfaction that it has properly archived and can recover a decade's worth of data. Then, a region-wide natural disaster impairs the headquarters *and* destroys the secondary facility holding the tapes needed for recovery.

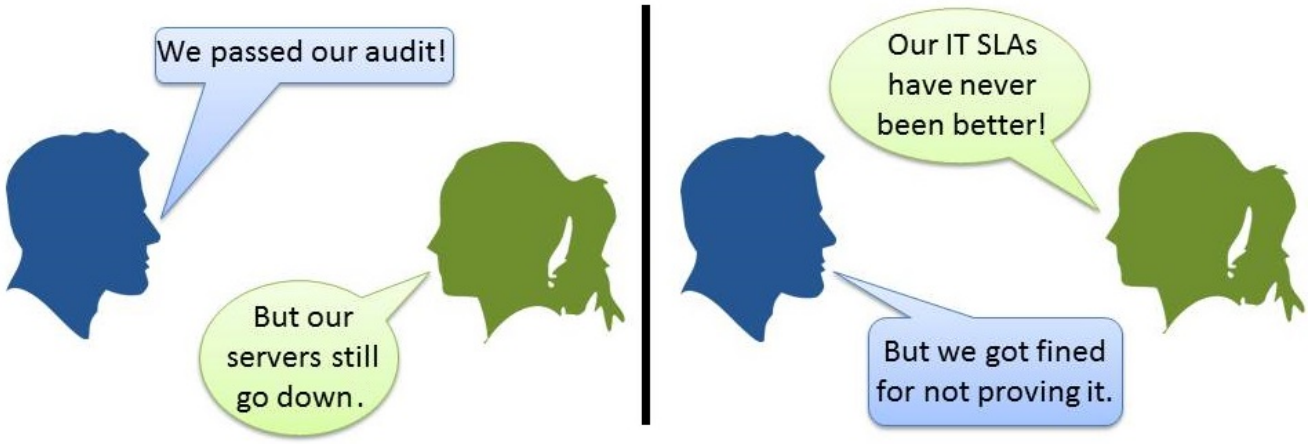
HOW A SOPHISTICATED, MULTI-TIERED DATA PROTECTION AND RECOVERY ENVIRONMENT CAN FAIL

Even sophisticated, multi-tiered data protection/recovery environments have failed audits because passing them requires more than just backup and recovery of data according to the in-house IT service level agreement (SLA). Here's an example. The IT team at ABC Company performed backup and recovery operations regularly, meeting all recovery point objectives (RPOs) and recovery time objectives (RTOs) defined in its SLA. The team shipped tapes offsite for safekeeping by a reputable service organization offering third-party backup storage. The team also engaged a managed service provider, leveraging it to replicate important data to the cloud automatically. Those steps and activities sounded great on paper and worked well in reality. But they did not ensure the company's regulatory compliance. And when the company faced an actual litigation event, no one could find the data that was being requested.

[3] Source: ESG Research Report, *Trends in Data Protection Modernization*, August 2012.

© 2013 by The Enterprise Strategy Group, Inc. All Rights Reserved.

Depending on the industry an organization is in, many overlapping regulations and jurisdictions might govern data protection and recovery. Again, these prescriptive regulations often define desired outcomes but in many cases are not comprehensive or detailed from an IT operations standpoint. Thus, meeting a requirement doesn't guarantee that an organization's data is properly protected.



Developing a data protection and recovery environment that meets organizational *and* regulatory requirements is more challenging than developing a data protection and recovery environment that meets only one of those requirements. Maintaining such an environment requires (1) an understanding of the capabilities of technology, and (2) an ability to interpret the regulations that apply to the organization's specific circumstances.

With committed collaboration among stakeholders, a balance can be struck that meets both the organization's and the auditor's needs. (And sometimes the balance absolutely has to happen, for example, in regard to maintaining customers' data privacy.) But in general, objectives and assumptions built into regulations that deal "generically" with data protection, retention, and recovery are not going to align 100% precisely, 100% of the time with what a specific organization needs out of its unique data protection, retention, and recovery environment.

A NOTE ABOUT "RETENTION"

The word "retention" has a different meaning to an IT administrator than it does to a records management specialist. To the records manager, retention of content is dependent on the organization's records retention schedules, not on a decision made based on an IT staffer's interpretation of regulations.

Understanding Compliance Regulations

Perhaps the most challenging part in ensuring that a data protection, retention, and recovery strategy is compliant with a particular regulation is determining what the relevant regulation is. That effort has to happen first. Step Two is figuring out how that regulation is "operationalized." To put it another way, Step Two involves investigating how the compliance inspectors are going to interpret the regulations when determining whether or not your organization is compliant.

Many pieces of legislation deal with topics related to data protection, retention, and recovery. The law or rule that applies can depend not only on what an organization does, but also on whom the organization does business with. And to make matters even more complex, legislation is subject to change. Factors that ensure compliance today may not apply tomorrow.

Although the following list of excerpts is not exhaustive, prominent pieces of current U.S. regulations relating to data protection, retention, and recovery include:

- **Section 11 of the Department of Homeland Security (DHS) Presidential Directive 20 (HSPD-20).** This section includes guidelines related to data backup (11.C) and securing additional resources for failover or rapid restoration (11.D). Section 16 of this document mandates that the DHS will develop continuity planning for state and local governments as well as private-sector critical infrastructure owners (16.F) and offer grants or potential funding for those agencies and operators (16.G).

© 2013 by The Enterprise Strategy Group, Inc. All Rights Reserved.

- **FEMA federal compliance directives covering the protection of vital records.** These directives certainly are applicable to data protection and backup mechanisms. Federal Compliance Directive 1 prescribes regular testing of high-availability and resiliency technologies.
- **Department of Defense Regulation DoD 5015.2-STD, specifically section C.2.2.9.** This regulation dictates that information backup and recovery/rollback capabilities are mandated for all executive branch agencies of the federal government, as well as the state agencies and contractors that interact with them.
- **HIPAA security section 2.3, rule 164.308 (a)(7).** This rule includes provisions relating to data backup plans, disaster recovery plans, and emergency mode operations plans—including business continuity, testing and revision procedures for those plans, and data and application criticality analyses.
- **Sarbanes-Oxley.** Under SOX, no mention of the terms "backup" or "disaster recovery" exist. But the regulation does contain substantial language pertaining to the retention of records to ensure sound business practices.

Many compliance regulations *mandate specific outcomes*, such as ensuring that recurring backups occur or that some form of disaster recovery capability is in place. They *do not mandate specific technologies* that would be suitable to provide that operational recovery or that can help ensure compliance with the directive in general. Even worse, the clarity of regulation is often compromised by the oblique and convoluted legal phrasing legislators use when they attempt to describe abstract (to them) IT concepts tied to business continuity and disaster recovery.

For an IT professional, the first step has to center on determining which specific regulations apply. A hospital network or a multi-campus educational institution will be subject to regulations that are different from the regs applicable to a financial services company or a firm that handles contract work for the Department of Defense.

The next step involves interpreting those regulations to determine what they require in terms of modifications to current data protection, retention, and recovery strategies and practices.

In some cases, putting those pieces together might be a job beyond the capabilities of an organization's existing staff. It may be necessary to have a trusted third party come in and spell out in detail what steps are needed to move an organization from its current data protection/retention/recovery strategy to one that is compliant with relevant regulations.

The Costs of Noncompliance

When IT professionals have to address "risk," they often think in terms of a concrete scenario such as "How do I ensure that I can

LAX COMPLIANCE CARRIES A HIGH PRICE

- The U.S. Immigration and Customs Enforcement (ICE) Office of Homeland Security Investigations imposed a $1,047,110 fine on a major American clothing retailer for violations of the Immigration and Nationality Act related to the employer's failure to verify the employment eligibility of its workers. The fine was the result of a November 2008 audit of the retailer's Michigan stores, which uncovered numerous technology-related deficiencies in the retailer's electronic I-9 verification system. Source: United States Immigration and Customs Enforcement news release, September 28, 2010.
- Data protection and enforcement top the list as the most costly noncompliance events. Although the average cost of data protection-related *compliance* was $3.5 million for a representative sample of 46 multinational organizations, the average cost to rectify *noncompliance* problems was nearly $9.4 million—an approximately $6 million difference. In terms of external compliance, the respondents reported that the most important and difficult requirements to comply with are those of the PCI DSS, various state privacy and data protection laws, the European Union Privacy Directive, and Sarbanes-Oxley. Source: *The True Cost of Compliance*, Ponemon Institute, January 2011.

© 2013 by The Enterprise Strategy Group, Inc. All Rights Reserved.

REGULATORY NONCOMPLIANCE has led to the loss of lucrative contracts, loss of jobs, reputational damage, and even incarceration. The negative impact can be on par with a natural disaster, and some companies that trade on their trustworthiness never recover.

restore this business-critical server to an operational state if its hard disks suddenly fail?" IT professionals' lives are filled with key performance indicators and benchmarks. They know when they are hitting their goals partly because when they do not, the functionality of some other business unit is impaired, and IT definitely hears about that.

Of course, backup and recovery can function like clockwork, yet compliance may still not be achieved. To lots of IT pros, the cost of noncompliance is mostly theoretical: Some of them even consider the idea that a backup and recovery solution could meet business but not regulatory needs as a contradiction … or as evidence of a problem with the compliance legislation. Some IT professionals and their management teams make compliance a priority only after they and their employers have experienced the pricey pain of noncompliance.

Being found noncompliant can lead to penalties, fines, expensive settlements, and revenue or market-cap losses. It may also involve costs that exceed the financial. In some cases, regulatory noncompliance has led to the loss of lucrative contracts, loss of jobs, reputational damage, and even incarceration.

If a good reputation depends on customers having faith in an organization's ability to protect data, and then that organization is found to be noncompliant, the negative impact to the organization can be on par with a natural disaster. Some companies that trade on their trustworthiness may never recover from a publicized finding that their data protection, retention, and recovery strategies weren't up to the standard mandated by legislation. For example, any company handling credit-card payments or medical records that is found to be lax in meeting legal standards for data protection, retention, and recovery will have trouble convincing clients that it should be trusted with that information again.

What to Look for in Regulatory Compliance and Retention

IT managers should note that although they might outsource data protection, retention, and recovery to a third-party provider, the responsibility for compliance does not transfer. The organization and perhaps specific employees with fiduciary or IT compliance responsibilities could be subject to punishment if the organization is found to be noncompliant.

Here's another reality that too many IT professionals and their managers don't realize: Cloud service providers provide comprehensive data *protection* and *recovery* options, but they often do not provide comprehensive data *retention* and long-term *archiving* options.

Some Specific Guidance About Offsite Archiving

To remain compliant, many organizations that use third-party cloud service providers also keep, in parallel, an off-premises archival infrastructure as a way of making sure that retention responsibilities are definitely being met.

Tape is usually the choice for this "cold storage" because of its appealing low-price/low-risk qualities. But whether the archived data is stored on tape or on other media, it may only ever be needed to prove compliance. Even if the data is *never* touched, when considering a parallel archival infrastructure, ensuring data survivability is paramount.

Some guidance:

- **Ship the archived data offsite to a secure location** and make sure it will only be in the possession of staff who should have access. Best practices in general and certain regulations in particular dictate that an offsite location should be some distance away from the location of the primary IT infrastructure.
- **Store the archived data in a manner that guarantees it will remain viable** as the source for recovered data throughout the regulated retention period. In other words, store it in a bunkered, climate-controlled, fire-

© 2013 by The Enterprise Strategy Group, Inc. All Rights Reserved.

protected, access-controlled environment. Data also needs to be stored on media that will remain readable for potentially many years after it is written to the storage. A good third-party vaulting custodian can make sure that the data is written to a "contemporary" media format—in other words, the custodian preserves the data using storage media that lends itself to remaining viable.

- **Ensure that the archived data is being indexed and cataloged properly.** If it becomes necessary to recover a certain piece of data, authorized staff must be able to locate that particular item in an appropriate time frame … and those time frames vary according to which regulation you are trying to adhere to.

A good rule of thumb is to look at the regulations relevant to your business and determine how quickly you need to be able to retrieve the information to be compliant. With DR, you have very short windows for recovery—minutes or even seconds. Conversely, when you're striving to comply with a retention regulation or responding to a litigation request, you may have the luxury of months or even years to produce the data. Weigh the risk versus the cost, and investigate whether tape may be a cost-effective yet reliable option to achieve regulatory compliance in regard to long-term data management.

Additionally, **chain of evidence is vitally important** at all stages of data movement, storage, and retrieval. Your recovery administrator must be able to attest that the storage media are in the exact condition that they were in when they were originally written to—i.e., that the data on them was never modified.

Retention Is "How Long" and "How Short"

When an IT organization is tasked with ensuring adherence to a comprehensive data protection, retention, and recovery strategy, that task includes making sure that the company is retaining data for the correct length of time. Often, this time period is dictated by a regulatory requirement.

If the organization is compliant, with an effective data protection/retention/recovery regime in place, then it's time to consider how accidental *over*-retention may also expose the organization to unnecessary risk. Just as consequences exist for failing to retain data for as long as the relevant regulations require, risks also exist associated with retaining data past its required retention period.

Here's a big reason why: All retained data is subject to legal discovery if a litigation or investigative event arises. It doesn't matter if the data's required retention period expired without the data being wiped.[4] And if the data was not deleted when it should have been, it remains "admissible." For lawyers, a key task in discovery involves asking, "Does the data still exist?" If the data was not deleted after it was no longer required, it is subject to discovery. On the other hand, properly deleted records cannot be used as evidence by attorneys or regulatory enforcers.

Organizations must retain data for as long as they are legally required to do so. No obligation impels any entity to retain data past the mandated period. Doing so offers no upside; it merely exposes an organization to potential legal or regulatory requests that would have been avoided if the data had been destroyed.

Put It in Writing—Data Expiration Policies

It's crucial to ensure, early on, that a high-level policy and granular step-by-step procedures are in place to deal with data older than the retention limit demands. Then, if litigators request that data, the organization can point to the policy to explain why it is unavailable. With no policy in place, litigators may assume the data exists but is not being produced. Additionally, any company that realizes it's been storing archival data too long and only deletes it when a discovery request arrives won't be looked upon charitably by the court.

[4] For an example of a regulation containing extremely granular, specific instructions related to retention periods, see the *U.S. Securities and Exchange Act of 1934, Rule 17a-4, Records to Be Preserved by Certain Exchange Members, Brokers and Dealers*, revised June 2004.

© 2013 by The Enterprise Strategy Group, Inc. All Rights Reserved.

Verifying Expiration

A new set of data will move into the "ready for destruction" category each day. Organizations that draft data-expiration procedures need to make sure they describe how they are verifying the destruction of that data.

IT IS A GOOD IDEA for organizations to take as much care in ensuring that their data is destroyed after the retention period expires as they took in retaining it per compliance requirements.

Destruction is not simply a matter of throwing tapes in a bin for a garbage truck to haul away. Organizations that deal with regulated, often sensitive data must ensure that (1) the destruction is verifiable, and (2) the data is not recoverable. Enterprising "Dumpster divers" with exceptional data forensics skills have recovered confidential data—including tapes and disks believed to have been destroyed beyond recoverability.

Data destruction is about ensuring that tapes, disks, and all storage media containing regulated data are disposed of appropriately. For example, sometimes, an internal hard drive will fail inside a production server that hosts a critical financial application. External retention regulations and a company's in-house destruction policy might require that the dead drive *still* undergo full destruction to ensure no bits remain forensically recoverable.

When developing an expired data policy, specify the method(s) of destruction explicitly. If you employ a third-party organization to destroy drives and tapes, confirm that they carry out their tasks as promised. Basically, it's a good idea for organizations to take as much care in ensuring that their data is destroyed after the retention period expires as they took in retaining it per compliance requirements.

STORAGE SERVICES PROVIDER Iron Mountain (*see next page*) offers Secure IT Asset Disposition Services to help organizations safely recycle or repurpose decommissioned data center assets such as servers, racks, storage systems, and networking components.

On that note, when writing the data destruction policy, it's important to ensure the data is destroyed in accordance with appropriate regulations. Must the media be shredded, crushed, burned, or perhaps overwritten seven times, then reformatted, then degaussed? In some cases, it is also necessary to be able to provide the chain of custody for any storage media that once held sensitive data. Similarly, it may be necessary for an official to sign a document attesting that he witnessed the device's destruction. All of those details should be spelled out in the policy.

Additional Considerations and Advice

A top-notch data protection, retention, and recovery strategy goes beyond ensuring that an organization is legally compliant. It also helps the organization be more resilient against unforeseen disasters.

This white paper has described plenty of guidelines and concerns. Here's some more guidance to keep in mind when defining, designing, and implementing a data protection, retention, recovery, and destruction strategy:

- Realize that unless you perform regular recovery drills, the recoverability of your data is only theoretically possible. Your recovery drills should include not just recent data, but "cold" data, too. You should be able to verify that you can recover data expeditiously—right up to the retention limit—before you have to prove that you can in order to comply with a discovery request.
- Replicate your data so that it is geographically dispersed. Many disasters strike regions rather than specific buildings. Replicating business-critical data to multiple locations and hosting key systems in multiple locations increases the chance that your organization will recover from a disastrous event.
- Take care to ensure the security of your backed up data. Backed up data needs to be as secure as production data. When using backup tapes, ensure that they are stored in an environment permitting them to be as functional in seven years as they are when first written.

© 2013 by The Enterprise Strategy Group, Inc. All Rights Reserved.

A Possible Answer?

Clearly, achieving compliance and readiness in parallel—an effort that includes recognizing the differences between the two concepts—is a task encompassing multifaceted considerations.

Iron Mountain is a company that has spent 62 years devising and patenting a portfolio of management solutions to store customers' vital records securely. Presently, the vendor operates approximately 1,000 storage facilities supporting more than 150,000 accounts in 35 countries.

But specifically in terms of operational readiness and regulatory compliance, do this vendor's offerings map well to (1) what IT organizations should be aware of, and (2) what IT should be doing in regards to compliance and operational readiness?

Iron Mountain Archival Tape Management

The Iron Mountain Archival Tape Management solution is a new service unveiled in 2013. It is intended to help IT groups manage the content that their organizations are required to save for long periods of time. With the launch of Archival Tape Management, Iron Mountain is educating customers that they have a new, more efficient way to access older archival/backup data—reminding them that tape continues to play a critical role because it is cost effective, greener than spinning disk, and physically durable, making it well-suited as the "vessel" for years or decades of safe retention. A 2012 National Energy Research Scientific Computing Center (NERSC) case study reported that automated tape systems have a reliability rating of more than 99.999%.[5]

IRON MOUNTAIN CLAIMS THAT ITS NEW BUNDLED SERVICE CAN …

Protect and restore backup media for the long-term: Restore data without the additional cost of maintaining legacy software and tape backup subsystems plus the staff required to operate these systems.

Help users to know what is on backup tapes: Easily identify what's on your backup tapes to make effective decisions about retention, destruction and restoration.

Enable users to: Quickly and confidently respond to internal and external information requests.

The Iron Mountain Solution

The Iron Mountain solution has three components—comprising two existing services and one new service:

BECAUSE MAGNETIC TAPE is cost effective, reliable, and secure, many organizations use it as a crucial component of their backup solution and often retain those tapes as a de-facto corporate archive. According to annual published statistics, approximately 24 million tapes are sold worldwide every year.

Offsite Tape Vaulting Services—Archival tapes are protected in highly secured, environmentally controlled facilities. This service also includes destruction of physical tapes that have been retired (as well as wiping and destruction of disk drives and other storage media), complete with a chain-of-evidence trail and a certificate of destruction that can be shared with regulatory auditors if needed.

Restoration Assurance Program—Restoration and migration assurance from Iron Mountain allows customers who are storing information for long periods of time to efficiently identify, restore, and deliver to other parties the data contained on backup media—regardless of the media's format or the original tape backup subsystem that was employed. This service also covers degraded-tape data restoration, and it includes migration of data stored on old tape formats to newer tape media if desired. That particular area of support means that Iron Mountain's customers can rid themselves of the obsolete tape backup subsystems that they have been keeping in the data center for years "just in case."

[5] Source: Mike L. Welcome, Storage Systems Group, National Energy Research Scientific Computing Center (NERSC), as reported in *InfoStor* Magazine, June 2012.

© 2013 by The Enterprise Strategy Group, Inc. All Rights Reserved.

Tape Catalog Manager—This is the new component of the Archival Tape Management offering. Tape Catalog Manager provides a single view of backup catalog data across heterogeneous tape backup subsystems, enabling faster turnaround for data-restoration requests. Popular backup software that is compatible with the Iron Mountain Tape Catalog Manager consists of Symantec NetBackup, EMC NetWorker, and CA ARCserve.

This offering is intended to appeal to companies that have accumulated several catalogs but want just one. The cataloging is sophisticated enough to allow Iron Mountain's end-user clients to map out which records and other information reside on which backup tapes, offering transparency into the tapes' content in response to an audit or an e-discovery request.

The premise is that storing information is fine, but if you can't find it fast when you need it most, it's still useless. Iron Mountain takes responsibility for hosting the catalog and locating the right electronic records during a regulatory investigation, thus allowing customers to retire their own cumbersome collections of (often-incompatible) catalogs that likely proliferated over time.

© 2013 by The Enterprise Strategy Group, Inc. All Rights Reserved.

The Bigger Truth

IT professionals and their managers need to be aware that there is more to a data protection, retention, and recovery strategy than being able to recover data and servers that are sitting on the production network or are functioning as the nightly backups.

Worldwide, a multitude of rules and regulations exist requiring organizations to meet various data protection, retention, and recovery benchmarks. Paying attention to these regs long-term is just as important as being operationally prepared day-to-day from a business continuity/disaster recovery standpoint.

The difference is that an abundance of products/services are being specifically marketed to handle all sorts of BC/DR activities, while the seemingly ever-growing crop of regulations rarely provide any guidance at all, much less specific product recommendations, as to how compliance should be accomplished.

The penalties for noncompliance are real, however, and they are sometimes quite specific. An organization found to be noncompliant can face fines, customer losses, and long-term reputational damage. To remain compliant, an organization needs to confirm that its regulation-related data is recoverable at all points throughout the mandated retention period. This means:

- Making sure any tapes holding older data are stored in a **climate-controlled, secure location** and are cataloged in such a way that data can be located quickly should it need to be recovered.
- Minimizing risk in another fashion, with organizations ensuring that **critical data is geographically dispersed**, so that the impact of a regional disaster is minimized.
- Organizations should have **data destruction policies** in place to lower risk even further, specifying destruction of data that no longer needs to be retained to meet compliance obligations. That destruction must occur in an appropriate, demonstrable manner.

Iron Mountain's newly beefed up Archival Tape Management solution has the potential to fit the bill for many compliance-exposed corporations, institutions, and public-sector entities. The vendor's expanded offering covers multiple bases—providing capabilities for quick recovery of information on tape archives, capabilities for moving away from legacy media or outdated onsite storage environments that are unsuited for compliance, and a way to do it all in a manner that reduces budget strains and lessens everyone's regulatory and operational-readiness worries.

© 2013 by The Enterprise Strategy Group, Inc. All Rights Reserved.

Enterprise Strategy Group | **Getting to the bigger truth.**

20 Asylum Street | Milford, MA 01757 | Tel: 508.482.0188 Fax: 508.482.0218 | www.esg-global.com