



Julie Marobella
Senior Research Analyst, Information Infrastructure Group

Storage and Compliance: Finding the Balance and Flexibility

May 2005

Companies are expending great effort on creating and formalizing regulatory compliance processes, policies, and procedures. IT solutions enter the picture when companies attempt to automate these compliance processes and make them sustainable. IDC believes that an information management for compliance platform will emerge in response to these efforts. This platform will focus on enabling companies to more systematically address compliance and risk mitigation across all IT and business practices. All these developments will fuel the growth of the information management for compliance market, which IDC believes will grow from \$7.5 billion in 2004 to \$20.5 billion in 2009, representing a 22% compound annual growth rate (CAGR). Storage will play a huge role in this market.

The following questions were recently posed by StorageTek on behalf of its enterprise IT management customers to Julie Marobella, a Senior Research Analyst in IDC's Information Infrastructure Group.

Q. The noise level around compliance is high today, and only seems to be increasing. How can companies address so many daunting regulatory requirements and still run their businesses?

A. The key is to step back from the commotion and focus on the three pillars of compliance: people, processes, and technology. Part of this focus will entail developing policies and processes that meet the common operational goals of an organization's line of business managers, its legal counsel, and its IT managers.

Integrating these operational policies across corporate constituencies will then help drive decisions about what data to archive and when, and enable operational managers to understand the full lifecycle of the information. They will know how and where information is created, how it is managed, who has access to it, when it needs to be stored, and when it needs to be archived.

It's critically important to recognize that "information" means *all* content created by an organization — structured content such as database files, and unstructured content such as emails, instant messages, and office files. Information should be defined as really any content format imaginable that holds business value, including images.

The other important action is to embed compliance processes into daily operations. Compliance processes cannot be adjacent to a company's operations; they must be integral to those operations. Otherwise the compliance will not be sustainable, and eventually the

company will find itself in regulatory trouble. This principle applies equally to storage operations; compliance is not a standalone or point solution. Compliance needs to be woven into policies and processes for archiving, backup and recovery, and overall business continuity strategy.

Q. What are the key things companies should consider when looking for a solution to their information management for compliance, as well as for their broader archive needs?

- A. The first consideration should be to build information management processes and articulate the policies and procedures that drive information retention and archiving. Again, if those policies aren't in place, then compliance efforts won't be sustainable. Articulating the policies and procedures, however, requires understanding how information is created in the company, as well as what information requires retention by law and how retaining that information fits within the company's IT and storage infrastructure (which must serve other business needs, too, of course).

However, this not an easy task. Compliance is very much a moving target from a records-retention standpoint. SEC 17A-4 requirements aside, records-retention regulations aren't yet fleshed out, and legislators and auditors will be focusing more on records retention in the future. In short, what companies must deal with today is not what they'll have to deal with tomorrow. Therefore an organization's storage architecture needs to be flexible enough to meet changing regulatory needs — and also scalable enough to meet broader business needs such as the growth of information needing to be retained, increased retrieval, recovery and discovery requests, and increased pressure for comprehensive data protection.

Another consideration is that regulatory compliance is forcing companies to retain much more information than they formerly did — not just standard records, but audit logs, security logs, and other internal-controls information. Therefore a best practice is to incorporate compliance requirements into the policies that dictate how various types of information is archived, but don't let that be the only factor. Incorporate the business value of the information into the policies such as the usefulness of the information to increase a company's knowledgebase, or to enable better decision-making and greater productivity. In other words, don't let this new internal-controls information languish in an archive system, but find ways to link it back to business improvement.

Q. Given that various regulatory and business demands can be conflicting, it seems difficult to satisfy all of them simultaneously. How do companies cope?

- A. IDC sees conflicting forces in two areas. The first is within external governmental regulations around data retention. For example, certain U.S. data privacy regulations and European privacy regulations contradict each other in terms of how long customer information must be retained. The second area is within a company's internal policies. For instance, legal and IT often disagree on email retention in terms of the business value, risk, and length of retention

Both these situations are challenging and few companies have found a comprehensive answer. The key to the solution is flexibility. By extension, there is no single piece of hardware or software that can resolve these compliance contradictions. It takes a storage architecture flexible enough to handle a variety of compliance policies. For example, suppose a company must keep information for a long time, but some of that information needs to be accessed aggressively, while other information needs to be vaulted away, protected from on-going operations and is very rarely accessed.

This is where a tiered-storage, policy-driven environment could leverage both tape and disk as complementary technologies. There are advantages to each medium, and if you need maximum flexibility, then you don't want to be viewing the question of tape versus disk as "either/or," but rather as two important pieces of a broader strategy.

ABOUT THIS ANALYST

Julie Rahal Marobella is a Senior Research Analyst in the Information Infrastructure group. Ms. Marobella is responsible for the newly-launched Information Management for Compliance research service, with a research focus on the areas of Document Management, Records Management and Compliance Infrastructure.

ABOUT THIS PUBLICATION

This publication was produced by IDC Go-to-Market Services. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Go-to-Market Services makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

COPYRIGHT AND RESTRICTIONS

Any IDC information or reference to IDC that is to be used in advertising, press releases, or promotional materials requires prior written approval from IDC. For permission requests contact the GMS information line at 508-988-7610 or gms@idc.com. Translation and/or localization of this document requires an additional license from IDC.

For more information on IDC visit www.idc.com. For more information on IDC GMS visit www.idc.com/gms.

Global Headquarters: 5 Speen Street Framingham, MA 01701 USA P.508.872.8200 F.508.935.4015 www.idc.com