WHITE PAPER
March 2005

Best practices in information lifecycle management for private sector compliance

ABSTRACT

Compliance is a significant component of a successful information lifecycle management (ILM) strategy. An ILM approach to addressing compliance can help you meet compliance requirements at the lowest possible cost. Understanding compliance issues and implementing compliance best practices within an ILM framework can help you reduce business risk while improving your competitive advantage.

1 Executive summary

Information lifecycle management (ILM) is a sustainable storage strategy that balances the cost of storing and managing information with its business value. A well-executed ILM strategy can result in a more agile organization, reduce business risk and drive down both storage unit and storage management costs. Information lifecycle management also provides a structure for dealing with new regulations by including the requirements they imply or specify for data classification, storage management policy and information placement. Regulatory compliance is a broad topic and this paper addresses only those aspects that deal with record retention and data storage. However, an ILM approach to addressing compliance requirements can help you meet those requirements at the lowest possible cost.

The ILM best-practices approaches to managing compliance requirements outlined in this paper offer other benefits. The approaches recommended can help you align IT with business priorities, clarify the linkage of business processes to data, optimize the use of existing storage infrastructure and enable a broad set of capabilities that will provide spillover benefits for all enterprise information.

While we have identified several best practices in this paper, a few key behaviors appear most important in providing lasting business impact:

- Treating compliance as simply an additional set of service level requirements, and integrating them into core ILM strategies and processes, will strengthen overall IT processes.
- Establishing effective interaction among legal, line-of-business and IT functions is essential to meeting compliance requirements, and will enhance business and IT alignment.
- Integrating compliance-driven data protection, archive/discovery and security requirements into information management services provided within a broad ILM strategy will facilitate a comprehensive approach to compliance requirements and provide expanded functionality across the enterprise.
- Integrating enterprise content management functionality into ILM to address compliance-driven discovery and records management requirements will enable this technology for broader application.

To meet compliance challenges efficiently in the long term, organizations need to incorporate a powerful combination of policies and tools into ILM. Complex requirements are being placed on the IT infrastructure, including the need for enhanced data protection capabilities, automated retention policies, and authentication and secure access.

Over time, most compliance requirements will become part of normal operations and not viewed specifically as compliance activities. Most organizations today appear to realize this and have found ways to meet compliance requirements within their existing storage frameworks. ILM provides a “best-of-breed” approach to doing this. Integrating compliance-driven requirements into an ILM strategy will enrich the ILM implementation, resulting in an optimized approach to overall storage management and will begin to move the overall business toward the capability to use knowledge for competitive advantage.

Compliance is conformity with some criteria, established by regulations or standards, or created by an organization based on business needs.

Information lifecycle management (ILM) is a sustainable storage strategy that balances the cost of storing and managing information with its business value. ILM provides a practical methodology for aligning storage costs with business priorities.

Information lifecycle management provides a structure for dealing with the requirements resulting from regulation.

2 The compliance issue

With the current level of hype surrounding compliance, a newcomer to IT might guess that it is a new phenomenon. In fact, U.S. businesses have faced compliance with local regulation since the beginning of the colonies, and federal regulation since the nineteenth century.

Though compliance is not new, it is fair to say that its notoriety has reached an all-time high. There are three primary drivers for the current level of attention to compliance:

- **Technology** — Certainly the business world was simpler when business records were on paper, kept as originals and locked in file cabinets. Today, records are stored electronically, and regulations exist to address the resulting issues, such as how to guarantee authenticity, provide reasonable accessibility and protect privacy.
- **Economics** — Recent economic conditions have exposed weak business practices. The late 90s boom and bust of the Internet economy and the recession of the early 2000s exposed several notable cases of either outright fraud or simply poor business processes. Legislators have responded quickly to the ensuing public outcry.
- **The Press** — Exacerbating both economic and technological factors, the press has made a major contribution to the current focus on compliance. Increased intensity and pervasiveness of media coverage has created additional pressure on government. While past business scandals have received media coverage, the demonizing of companies and executives is a new trend that parallels the public's fascination with celebrity of any kind.

Within its broad framework, information lifecycle management (ILM) offers an approach to managing the impact of regulation. ILM links business intent with storage management activities to align the business value of information with the cost of storing it. Complying with regulations adds another set of requirements to the process of managing information, affecting three major areas of ILM: data protection, archive and discovery of information, and privacy.

ILM-based compliance integrates the business rules that define compliance throughout the layers of the ILM logical model, linking business intent with storage management reality.

Compliance:

- *Extends data classification*
- *Broadens policy requirements*
- *Forces the integration of ILM and content management*
- *Adds requirements to placement and movement capabilities*
- *Expands the capabilities necessary in the storage infrastructure*

3 Information lifecycle management role

Information lifecycle management provides a structure for dealing with requirements imposed by regulations or defined from within the business.

The ILM logical model provides a framework for understanding the process of transforming business intent into storage management reality. It begins with the business interface defining the relationship of IT and business processes. A business value integration layer provides the linkage between business processes and storage management, tying business processes to policy and data classification. A storage management integration layer links intended actions and the actual outcomes of storage management actions. It includes resource management, metadata management and measurement functions. An information placement layer integrates activities that optimize data location, including data protection, retention management and storage optimization. Finally, the physical infrastructure, consisting of the physical hardware and software, is used to store data, interconnect storage and servers, move information, and monitor and manage storage.

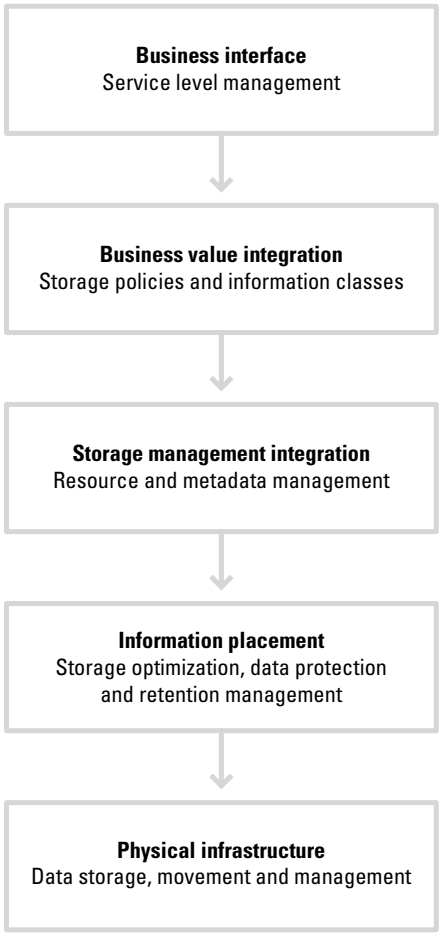

Figure 1. ILM logical model

ILM/compliance best practices:

- *Treating compliance as simply an additional set of service level requirements and integrating them into core ILM strategies and processes*
- *Building effective interaction between legal, line-of-business and IT functions is essential to meeting most compliance requirements*

The impact of compliance with regulations in the above logical model is relatively simple:

- Compliance extends the richness of data classification, adding additional criteria and data classes to the schema.
- Compliance requires broader policy functions, including enhanced retention/disposal management and assignment of information to specific infrastructure elements.
- ILM-based compliance forces the integration of enterprise content management (ECM) and rich metadata to allow for efficient discovery of archived data.
- Compliance adds requirements to placement and data movement capabilities to ensure new policy functions are implemented.
- Finally, compliance extends capabilities necessary in the storage infrastructure to include special data protection capabilities (e.g., write once, read many, or WORM) and object-oriented or content-addressable storage.

The key impact of compliance on ILM is the need to ensure that the ILM model evolves to a higher level of "richness," including rich data classification, rich policy, rich metadata and rich infrastructure. In doing so, ILM-based compliance will provide a broad spectrum of spillover benefits that can extend to all enterprise information.

4 ILM/compliance best practices

1. Treating compliance as simply an additional set of service level requirements, and integrating them into core ILM strategies and processes, is a sound best practice.

We find no reason why external regulations must be handled in an extraordinary manner; in fact, we find many reasons why they shouldn't be. While the requirements are often vague and confusing, the fundamental ILM practice of defining service level agreements and translating them into storage management actions should encompass compliance requirements. The strongest reason for doing this is the value inherent in the core concepts of quality and process.

Compliance requirements should not be surprises; the regulations typically go through a laborious review and codification process. There should be little need to react quickly with costly add-on processes that are likely to be incomplete and inconsistently followed. Leading companies track pending requirements and implement systems that can incorporate new compliance requirements into existing processes in an orderly manner.

When ILM processes are well-designed and implemented, staying within their constructs to handle additional requirements is merely good business sense.

2. While some regulations are written specifically with new technical capabilities in mind, sound internal polices can reveal alternatives that allow for even greater efficiencies, flexibility, or opportunity while meeting requirements.

Effective interaction among a company's legal, line-of-business (LOB) and IT organizations is key to recognizing these situations. Legal and LOB should work together to research requirements and agree on risk-balanced requirements. LOB management and IT should work together to define service level agreements incorporating compliance requirements. Finally, IT should define service objectives and solution alternatives that solve technical needs.

ILM/compliance best practices (continued):

- *Understanding that compliance is not only archive or records management, but is a much broader concept, including:*
  - *Data protection*
  - *Discovery of stored information*
  - *Privacy and security*
- *Integration of compliance-driven data protection requirements and capabilities within a broad ILM strategy*

A comprehensive ILM strategy that accepts business direction via service agreements, defines data classes to accommodate requirements and enforces policy to enact requirements can accommodate compliance needs.

3. It is important to understand that compliance with regulations is a broad concept that goes beyond archive or records management.

Despite some of the messages being delivered to the market today, compliance-related information management needs are multifaceted. Compliance is far more than records management. Most regulations, standards and adopted compliance practices drive service level requirements in three categories: data protection, discovery and privacy.

- **Data protection** — If data is not recoverable to begin with, then superior records management solutions have little meaning. This is one reason that some regulations, like the Health Insurance Portability and Accountability Act (HIPAA), specify data protection processes, including backup and recovery.
- **Discovery of information** — Regulations often specify the retention time, required provenance and storage approach for specific types of information, and require organizations to present information in a timely manner for the purposes of legal discovery.
- **Privacy** — Some regulations specify requirements for privacy and access control to information. Most often these regulations relate to information held by organizations about individuals, e.g., customers or patients.

4. Sound data protection capabilities are critical to complying with regulations.

Some regulations, like the Gramm-Leach-Bliley Financial Services Modernization Act, include requirements for specific data protection capabilities. Other regulations simply include general requirements that information must be available and thus must be protected.

Generally, attention to compliance has increased the length of time information must be retained. Extended retention periods increase the possibility of storage media degradation and the potential for human error. Tools that automate data protection, allow for efficient backup of data and facilitate migration of data to new media as access requirements change over time are needed. Integration of compliance-driven data protection requirements and capabilities within a broad ILM strategy is clearly a best practice.

5. Enterprise content management (ECM) systems, coupled with a sound ILM strategy, are critical to accessing needed data in a timely manner while storing it in a manner commensurate with its business value.

Tracking the location of every potentially relevant record to meet compliance requirements is increasingly challenging.

ECM applications have value well beyond serving regulatory requirements; they are a good example of technologies that can facilitate meeting compliance needs while also providing broad competitive business advantage. For example, access to effluent release information might also facilitate improving production efficiency. Even if none of the data required to meet regulations is useful for other purposes, the tools selected to manage that information are usable for other business data.

ILM/compliance best practices (continued):

- *Integrating enterprise content management functionality into ILM as a service to address compliance-driven discovery and records management requirements*
- *Integrating security and access control as part of the ILM data classification schema and policy, and imbedding it as an ILM service*

Regulators often have the right to request information on the basis of unpredictable criteria. For example, e-mail and other records may be requested based on who created or received them, or a combination of search words. Under regulations like the Food & Drug Administration's 21 CFR Part 11, records must be searchable in such a manner, and all data access and change records must be maintained. In some cases, it is difficult to determine or predict what information must be discoverable. For example, the Environmental Protection Agency's Toxic Substances Control Act calls for keeping files based on the imprecise criteria of potential for "allegations of significant adverse reactions." High-function, flexible tools and processes are required to meet such information requests.

Some vendors have chosen to interpret vague discovery regulations to their advantage. For example, some have implied that storage technologies with millisecond access times are required to meet the many regulations stipulating ready access to data. In fact, the intent of these regulations is to insure that information retrieval does not delay investigations. Access to data within a few minutes versus a few milliseconds is not significant in this context. The multiple, highly-publicized examples of companies failing to meet regulators' information requests on a timely basis typically resulted from issues with discovery capabilities, not hardware access speeds.

Effectively implementing enterprise content management as a service in a tiered ILM implementation provides a means to balance the cost of meeting discovery needs with the business value of information.

6. Integrating security and access control as part of your ILM data classification schema and policy, and imbedding it as an ILM service serves compliance, but is a best practice on its own.

Some of the most valuable records stored by companies include personally identifiable information about individuals. Commercial use or inappropriate disclosure of that information raises new concerns about privacy. Some of the regulations create conflicts between disclosure, effective business use of information and privacy.

Financial services companies are faced with the difficulty of having to retain — but not inappropriately use — customer information. For example, they must meet disclosure requirements in the Patriot Act to combat terrorism, and concurrently comply with regulations covering proof of non-discriminatory business practices.

In healthcare, companies must guard against negatively impacting quality of care as they implement the elaborate access control and data protection required by HIPAA.

7. Responding to requirements imposed by regulations should be handled within the framework of ILM as "business as usual."

However, it is important to recognize the need for some specific services and capabilities:

- **Write once, read many (WORM) storage** — In general, regulations do not specify WORM storage capabilities. Some, like the Securities and Exchange Commission's 17 CFR 240.17a-4, do require that certain transaction records and customer correspondence be kept "exclusively in a non-rewriteable, non-erasable format" (i.e., WORM). WORM capabilities are an important service that will definitely augment an ILM strategy, for both specific regulations and in general, as a sound business practice for critical archive data. Integration of WORM capabilities as an available ILM service, deployed based on data classification and policy, provides a solution that both meets general business needs and serves compliance.

ILM/compliance best practices (continued):

- *Business as usual with some exceptions:*
  - *WORM*
  - *Object-oriented and content-addressable storage*
  - *Migration planning for technology refresh*
- *A cost-effective compliance strategy may include taking a mass-customized approach to compliance by broadly adopting the requirements of the strictest regulations that apply to a part of an organization's information.*
- *Understanding and adopting input from industry standards groups*

- **Object-based storage** — Object-based storage systems, also known as content-addressable storage (CAS) solutions, essentially associate metadata (the information about a file's characteristics) with the file's physical location on the storage media. Metadata information in electronic records defines important attributes, such as authorship, history of edits and dates of creation. ECM software can contain the business intelligence to attach retention characteristics to the data and move it between different tiers of storage based on defined policies. For example, infrequently accessed data can be stored on tape and retrieved quickly through a metadata index that resides on disk. The ECM system can provide that data entering the archive is retained for the specified retention period and that it is not altered during that period.
- **Migration planning and technology obsolescence** — Extremely long retention periods imposed by some regulations (for example, HIPAA) create special problems. When combined with WORM requirements, the problems are particularly difficult. ILM services must be applied to manage technology refresh in a manner that extends the lifecycle of information beyond the lifecycle of specific technologies, and still meets compliance requirements by providing authentication and managing audit trails for migrated data.

8. A cost-effective compliance strategy may include taking a mass-customized approach to compliance by adopting the requirements of the strictest regulations that apply to a part of an organization's information.

Literally thousands of potentially conflicting inter-country, federal, state, local and professional laws, regulations, mandates and standards govern or may apply to any given organization. The cost/benefit analysis of adding data classes and polices may result in the application of standards that are more stringent than is legally required. Some analysts refer to this practice as the use of a "gold standard" and cite Department of Defense Directive 5015.2 (DoD 5015.2) as an example of a standard that is frequently used.

9. Understanding and adopting input from industry standards organizations can mitigate compliance ambiguity.

Standards boards often buffer the vagueness of regulations and are serving an increasingly important compliance role. For example, as organizations struggled to understand the implications of Sarbanes-Oxley, many companies' auditors turned to a standard from the American Institute of Certified Public Accountants, Statement of Auditing Standards No. 70, as a means of validating that they were collecting and maintaining financial records in a reasonable manner.

Standards organizations may also create standards in an attempt to reduce the need for additional government regulation. The Environmental Protection Agency specifically mentions the International Standards Organization's ISO 14000 as a means of avoiding the need to demonstrate compliance with more specific regulations. The trend of regulations specifically mentioning standards as a means of meeting or avoiding more onerous regulations is likely to continue.

The advantages of taking a standards-based approach to meeting compliance requirements include the tendency of standards organizations to focus on defining practices based on driving business efficiency and incorporating process methodologies.

ILM/compliance benefits:

- *Process integration drives adaptive IT*
- *Enhancing business/IT alignment*
- *Storage optimization, including compliance information storage*
- *Enterprise content management and rich metadata spillover benefits*
- *Leveraging compliance-specific capabilities*

5 Benefits of managing compliance within an ILM framework

Integrating the requirements imposed by regulations into a comprehensive ILM strategy provides several benefits. An ILM strategy that encompasses compliance can help to accelerate the implementation of ILM across all data classes and policies, reduce overall IT storage costs and drive best practices into the entire IT infrastructure.

One of the key benefits of using an integrated ILM approach to compliance is the ability to adapt to new regulations. A process-based approach to integrating new requirements serves many other IT initiatives and drives IT flexibility. Adaptive IT organizations adjust rapidly to business change and can drive competitive advantage through IT excellence.

Compliance can provide the impetus to better align business and IT. Integrating the requirements imposed by regulation will formalize the relationships between legal, audit, finance, line-of-business management and IT. The side benefit is that these relationships will enhance the quality of service for all business processes.

An ILM approach to compliance that includes the implementation of tiered storage and optimizes the use of storage infrastructure enables compliance information to be stored in a way commensurate with its value. In doing so, compliance provides the means to store all archived data in the most cost-effective manner.

The rich metadata approach that ECM solutions drive is a key best practice in meeting compliance requirements. Here again, serving compliance requirements provides benefits that spill over to the rest of the organization's data, providing advanced data mining and warehousing functionality for all appropriate enterprise information.

Finally, even the "exceptions to business as usual" that compliance drives (WORM, object-oriented storage or CAS, and sophisticated technology refresh planning) can be leveraged across the organization.

A comprehensive ILM strategy that accepts business direction via service agreements, defines data classes to accommodate requirements and enforces policy to enact requirements can accommodate compliance needs and provide a model for introducing the benefits of enriched ILM to the entire enterprise.

ABOUT STORAGETEK®

Storage Technology Corporation (NYSE: STK) is a $2 billion global company that enables businesses, through its information lifecycle management strategy, to align the cost of storage with the value of information. The company's innovative storage solutions manage the complexity and growth of information, lower costs, improve efficiency and protect investments. For more information, visit www.storagetek.com, or call 1.800.275.4785 or 01.303.673.2800.

WORLD HEADQUARTERS

Storage Technology Corporation
One StorageTek Drive
Louisville, Colorado 80028 USA
1.800.877.9220 or 01.303.673.5151

JT 0010 A 03/05