

Implementing a Compliant ILM™ Solution

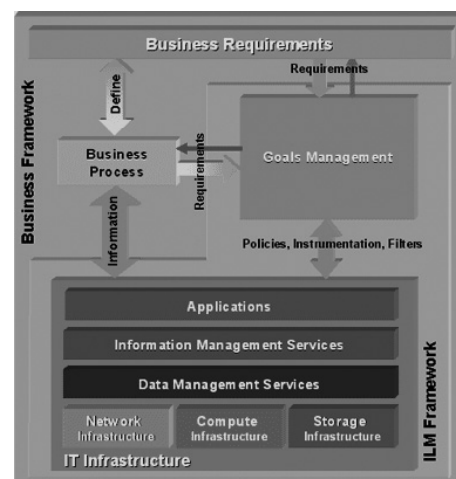
There's no question that Information Lifecycle Management (ILM) is a hot topic in the information storage industry today. But what exactly is ILM?

Gartner defines ILM as optimizing the cost of storing, protecting, retaining and recovering information for all of a company's necessary records, whether electronic or hardcopy. Put more succinctly, ILM is a concept for dynamically managing data over its lifecycle, from creation to deletion, as its value changes over time.

But is that a new concept? Not really. ILM is all about data storage, cost optimization and storage management policy, which is not that different than Hierarchical Storage Management, or HSM, which has been around for decades. HSM gives IT departments the tools to manage the expense of data storage based on its importance, where importance is defined as frequency of access. Under that scenario, information is relegated to back-up tapes as it ages and its use declines. This is fine from an IT perspective, but doesn't address potential business issues, and this is where Compliant ILM™ comes in.

What Compliant ILM™ or cILM™ brings to the table is a melding of business concerns with IT capabilities. Today, if you were to ask who in your company is responsible for defining business requirements to assess risk, the chances are that your IT staff would not feel accountable. Nor would they be the group to define the regulatory business practices that deal with compliance mandates instituted by the federal government. The IT organization would, however, enthusiastically embrace the role of implementing an Information Lifecycle Management process.

We can better understand this bifurcation between business issues and technology solutions by looking at the Storage Networking Industry Association (SNIA) definition and model, which clearly segments the business requirements of compliance and the implementation responsibilities of IT. Under their model, IT owns responsibility for delivering the lowest storage TCO (Total Cost of Ownership) and the operational processes that support business transformation, but it is the business side of the house that creates the foundation on which Compliant ILM is built. Compliance, after all, is a business requirement concerned with assessing risk, defining needs and developing the processes that deliver business value; it is not an IT problem.



Source: Storage Networking Industry Association

ILM is a business problem with legal ramifications, and IT's role is to support its implementation, not define it or fund it. In fact, most IT organizations lack the budget required to implement Information Lifecycle Management.

THE ORIGINS OF COMPLIANT ILM™

Seeking to ease investors' concerns over fraudulent accounting practices and general corporate mismanagement, the U.S. government introduced risk-management obligations in the late 1990s that affect CFOs, CIOs and CEOs. There are punitive measures associated with non-compliance, and a burden has been placed on operating managers to institute processes, technology and employee training to ensure compliance.

Simply put, Compliant ILM™ meets business and regulatory requirements for data retention and access. And while regulations like Sarbanes-Oxley were imposed in the U.S. in response to failures in corporate governance, the reality is that legal and regulatory compliance issues span the globe, from the smallest company to the largest enterprise.

It is also a reality that ILM and compliance are not separate concepts. Both are programs that employ a combination of technologies and processes to address the importance of information to a business at any point in time.

Compliance mandates such as Sarbanes-Oxley, or SOX for short, specifically outline the expectations government regulators have for corporate behavior, and reinterpretations of the SEC Act of 1934 clearly define the data retention policies and procedures that companies must follow in order to comply with regulations.

SOX requires publicly-traded companies to retain audit records capabilities for seven years, and the IRS and HIPAA require compliance with similar regulations. Today, there are over 10,000 local, state and national regulations to contend with, more litigation with discovery of any and all information related to a case.

So now the question becomes, is your enterprise in compliance with government mandates? In 2001 when New York State Attorney General Eliot Spitzer began his investigations, about nine billion e-mails were sent every day, and e-mail was not yet categorized as a "record." Then came the Enron scandal and Andersen Consulting's involvement, and the rest is history. Today, significant legal issues are associated with implementing a Compliant ILM™ solution.

While compliance concerns have pushed data retention into the spotlight, the necessity of meeting legal, tax and operational requirements has always been an important business issue. All enterprises must define and enforce data retention policies in order to comply with regulations like SOX, HIPAA, SEC 17a-4, and so forth, which means not only keeping data but also having the ability to search for and access relevant information.

The good news is that the processes and costs associated with implementing and maintaining a proactive compliance plan are relatively predictable, and the penalties associated with non-compliance are also well documented. With this information, ROI can be defined and implementation of a corporate-wide "proactive" compliance solution that addresses SOX or any other regulatory mandate can be initiated.

DEFINING THE KEY VALUE OF COMPLIANT ILM™

The decision to adopt a Compliant ILM™ approach begins with assessing the cost of compliance versus the risk of non-compliance.

The first insight is to recognize that federal government regulation of business practices in any industry results in some percentage of profit becoming an expense. Controlling the size of that expense is often an exercise in balancing efficient management practices with cost-efficient technologies.

So the crux of the issue is to define the business value of linking the information management challenge with technology that enables a Compliant ILM infrastructure, one that is both proactive in its foundation and reactive in its readiness solution.

Begin by developing a policy to govern the review, retention and destruction of both paper and electronic documents created or received in the course of business, keeping in mind that retention of some records is mandated by law.

Without a defined policy, the retention of all records or the destruction of relevant documents are equally troublesome, and may lead to lengthy and expensive “discovery” battles in litigations that might otherwise be avoided or economically resolved. Lacking firm definitions regarding the routine destruction of unnecessary information creates enormous volumes of records that must be searched, sorted and reviewed in response to discovery requests.

THE THREE-STEP PROCESS FOR IMPLEMENTING cILM™

There are three steps for successfully implementing an Information Lifecycle Management program, and there are also three steps to implementing a Compliant ILM program, although they differ slightly in sequence.

ILM begins with *data classification*. Incumbent in data classification is a thorough understanding of the data used by each application, by each business, and by each business user. Managers need to first determine the value of various categories of information and then define protection, movement and retention policies based on those relative values.

Once those valuations are set, seek input from the businesses and the users. Keep in mind that no single group will have a full sense of what can or ought to be done: Functional personnel will have the best sense for their particular business process and application requirements; IT personnel will have the best understanding of technical issues and ramifications; executives and legal counsel will want to provide input and direction with respect to regulatory and legal requirements.

Only when data retention requirements are addressed from a business perspective, from a financial perspective and from a legal perspective can policies can be enacted that migrate, protect, retain and eventually discard information based on business requirements.

The second step is to assess the *funding* necessary to implement an Information Lifecycle Management program, beginning with initial implementation through the ongoing investment necessary to retain corporate records throughout their required retention periods.

The final step is to secure senior *executive commitment* - from the CIO, from the CFO, from the chief legal counsel and from the operational business units - because implementing Information Lifecycle Management cuts across all these organizational boundaries.

THE BUSINESS VALUE OF COMPLIANT ILM

Compliant ILM uses a two-pronged approach - a sturdy foundation that supports a proactive “go forward” look to the future, and a reactive readiness solution that looks backward into the past. These processes address the two threats of regulation - demonstrating that current business processes are in compliance (proactive), and responding to eDiscovery litigation (reactive).

The “sturdy foundation” supports proactive business processes with an aggregate of governance policy setting, requirements inventory, and facts. In this foundation, senior individuals from a variety of backgrounds representing a cross-section of functions become the stakeholders that make the rules, define the risks and develop the policies. The requirements inventory defines the regulations, laws and policies that affect the enterprise. And the “facts” define the classification, retention timeframes and disposal process for various types of information. These aggregate definitions then become the cILM capabilities that are implemented by the IT organization.

Developing a proactive, sturdy foundation that supports a Compliant ILM implementation is, like the ILM process, a three-step procedure:

- Step 1 is all about policy development, where stakeholders develop governance rules that define information controls regarding use, retention and destruction.
- Step 2 develops the requirements inventory, identifying the data used in the business, categorizing various types of business records, and defining regulations, laws and policies.
- Step 3 creates the retention schedule based on the facts around information classification, retention and disposal as defined by the stakeholders - how long information must be retained, in what form, the degree of accessibility required, and the disposal time and type. This step also addresses cILM education, training and compliance and oversight.

Once an organization has the structure in place, then it's the job of IT and the records management group to translate this information into policies for hard copy and electronic information.

The following definitions provide perspective on the planning and decision-making processes behind the development of a Compliant ILM policy:

- Retention - Should the information be retained for a specific time period based on corporate governance or regulatory requirements?
- Disposition - Once the retention cycle is complete, should the information be disposed of completely or archived to a lower-cost media? Does the information need to be electronically shredded after the retention cycle has expired?
- Archiving - Should the information be archived for long periods? If so, must the archive be stored separately from the original?
- Recovery - How quickly must the information be recovered?
- Security - Will compromise of the information at different points in its lifecycle affect the business?

So far we've focused on the business value of Compliant ILM as it applies to proactively defining the lifecycle of various types of business information. But what about reactive readiness, such as a compliance audit or discovery request that seeks information related to litigation?

Electronic back-up and recovery media are fine for file and application recovery, but not for subject, or context, recovery. According to Computer Forensics, discovery searches can cost of to \$2,500 per back-up tape, with a single tape containing as many as 40,000 e-mails, and a single search costing upwards of \$90,000.

Advance preparation is key to effectively managing the cost of responding to electronic discovery demands, and can be critical in proving that the cost of a discovery should be borne by the requestor. The first step, as outlined previously, is to develop and implement a reasonable document management and retention policy with the involvement of all stakeholders - legal, IT, administrative, human resources, library and executive personnel.

For maximum effectiveness, adoption as a business policy with executive management support, clear documentation and ongoing personnel training are critical. Monitoring adherence will be powerful evidence during any discovery dispute regarding the destruction of documents prior to litigation.

A typical Fortune 500 company has in excess of 100 non-trivial lawsuits pending at any one time, all involving record retention and retrieval in compliance with legal discovery requirements. And this is a driving force behind the adoption of Compliant ILM programs.

Collecting the electronic documents such as e-mails, letters, memos, and spreadsheets that are relevant to a pending dispute can be complicated and expensive, especially if not planned and carried out efficiently. The sheer volume of available information, its geographic distribution and the technical complexities of the systems on which it is housed can create daunting obstacles.

THE COMPLIANCE COST/BENEFITS BALANCING ACT

For businesses that operate in a highly regulated sector, litigation or government investigation is a constant presence, and has become a significant risk-management issue for “C-level” executives. Due to the punitive measures associated with non-compliance, this can become the largest cost associated with compliance. However, with a proactive, sturdy foundation for compliance in place, business stakeholders can develop a plan that makes the associated costs relatively predictable, thereby minimizing your exposure. The cost associated with regulations such as the SEC Act of 1934 is straightforward as are the well documented penalties for non-compliance.

However, it is equally important to understand the organizational impact of compliance. It can disrupt a business and cause IT organizations to focus on resolving issues unrelated to normal business operations. Since profitability is the top priority for most corporations, this impact is best measured as an organizational cost or in the expense line of the income statement.

Some organizations may choose to ignore the compliance mandates, choosing instead to risk incurring the expense of non-compliance in hopes that compliance directives will be relaxed. Other organizations are resource constrained, unaware, or believe that the worst will never happen to them.

Non-compliance is not an option in an environment created by a lawsuit against your company or as a result of a regulatory investigation from the federal government. In these cases, civil penalty or lawsuit are likely scenarios, along with an unfavorable impact on stock price and negative publicity, or worse.

A discovery request associated with electronic information will cover timeframes, people and topics, and require an IT organization to locate and aggregate the relevant information. Even in a large IT infrastructure, only a subset of the relevant data resides in a management and data retention system; the balance resides on the network, on individual computers, and on backup tapes. The process of aggregating electronic information in response to a discovery request requires adherence to specific procedures governing data preservation and tampering. Lack of adherence to these processes can result in immediate penalties.

Companies will incur significant costs to comply with such a situation and only through a reactive readiness solution built on a sturdy foundation for compliance will they know what their costs are and proactively manage them. Despite the fact that organizations often ignore these costs as the “cost of a lawsuit” or as legal expenses related to the defense of the suit, the cost of compliance is very real.

The business benefits behind a sound Compliant ILM policy are in deriving maximum value from information while minimizing the IT cost of storage and management as well as the operational cost of compliance.

The goal is to strike the optimal balance between meeting business requirements and minimizing information costs - in other words, the right service level for the right data at the right time with the right business processes. This is the balancing act.

EVALUATING A cILM SOLUTION PROVIDER

The most significant criteria in evaluating a cILM solution provider are the vendor's stability and ability to execute. A very strong cash position and well-established market position, along with reputation, experience and commitment, are all important as well.

Vendors that are financially strong and committed to serving the market are very important because the worst-case scenario for an archive or a vault is that the vendor goes under, leaving the client to retain and recover their records - a very costly and painful exercise.

As for experience, a demonstrated capability in the retention and recovery of data, whether electronic or hardcopy records, is critical in selecting a cILM service provider.

In addition to establishing rules and policies for the retention of e-mail records, attention must be paid to unstructured data as well as structured data, along with database and relational data. The right vendor will have experience in each of these areas and will understand the differences in retention and access.

SUMMARY AND KEY RECOMMENDATIONS

Implementing Compliant Information Lifecycle Management is not a one-time activity, but involves both a long-term commitment and an ongoing program that is best planned in incremental steps. A two- or three-year Compliant Information Lifecycle Management project should be segmented into a series of six-month projects that will demonstrate success over a period of time. And a long-term, ongoing effort will require executive commitment within the IT organization.

Moving forward requires selling the value of Compliant ILM and records retention to the chief legal counsel and business unit executives, because this is where the return on investment is most likely to be, and this is the source of funding for the initial project and ongoing maintenance.

IN SUMMARY

- Segment the project into multiple steps.
- Demonstrate the value of implementing Compliant ILM, from initial archiving, records retention and secure storage, through information maintenance and ultimately deletion.
- Since profitability is “top of mind” for corporations, the impact of compliance is best measured by its impact on organizational costs and the expense line of the income statement.
- Establish senior management and executive support within IT.
- Secure funding commitments from the chief legal counsel, the chief financial officer and the leaders of the business units.

A good starting point is to affirm the readiness of a Compliant Information Lifecycle Management program by considering the following questions:

- Does your business have a comprehensive retention schedule that covers all media?
- Are your employees trained on information management policies?
- What types of litigation holds might be put on your information, and is there a process for exceptions?
- What is your disposal policy, and how does it apply across media?

With these and other system “health checks,” you can arrive at a recommendation for moving forward with a cILM implementation that will support reactive readiness and proactive compliance with today's information management requirements.

In the words of a Gartner market trends report on Storage Professional Services in North America, “Despite the differences in how individual companies define ILM, there is one profound common thread among them all. Namely, services will be key to the success of any ILM implementation. Without defined services to link ILM to business value and road map and implement solutions, there is practically no chance of widespread ILM adoption.”