8 Steps to Effective Information Lifecycle Management

Melissa G. Dederer, IGP, CRM, and April Dmytrenko, CRM, FAI

The need for an effective, compliant approach to managing information throughout its life cycle becomes very evident when a major event occurs, such as a lawsuit, an audit, a merger, an acquisition, or a divestiture. Without it, even daily business decision-making can be greatly compromised.

An organization that does not have an information lifecycle management (ILM) program will receive significant, long-term benefits from developing and implementing one, including:

Improved Availability – "Information age" employees must be able to find and access needed information quickly and be confident that it is the right information. ILM gets the right information to the right people (those who have the right to access it) at the right time.

Reduced Risk – By implementing an ILM approach, the organization has less information to manage, which reduces the risk of basing important business decisions on outdated or incorrect information. It also means there is less information to produce in a legal or regulatory investigation, which reduces the risk of exposing information.

Reduced Costs – Eliminating unneeded information reduces both electronic and physical storage costs. It also helps control the exponential growth of information and reduces overall operational costs by enabling employees to be more efficient.

Optimized Business Efficiencies – Having smaller volumes of information results in faster and more efficient searches and retrievals. Productivity will increase and, overall, the organization will be more effective.

Defining ILM

The information life cycle begins with information's creation or receipt; progresses through its organization and storage, retrieval, use, and maintenance with proper protection and preservation; and ends with its disposition. *Disposition* usually means destroying information, but it can sometimes mean permanently retaining it, based on the organization's retention schedule.

ILM is accomplished by strategically applying policies to manage throughout its life cycle all information – not just *records*, which *Glossary of Records and Information Management Terms* (ARMA TR-22-2012) defines as "any recorded information, regardless of medium or characteristics, made or received and retained by an organization in pursuance of legal obligations or in the transaction of business."

ILM includes determining:

- What information the organization has
- Where it is stored
- Who has ownership and/or accountabilities for it
- Why it is being retained
- How quickly and easily it can be accessed
- How it is tracked
- How long it must be retained

A best practices approach that will ensure success in developing and implementing an ILM program is supported by the following eight steps.

Step 1:
Learn About the Information

The first step in developing and implementing ILM effectively is to learn the 5 Ws and H – What? Where? Who? Why? When? How? – about the organization's information. Although these questions sound simple, finding their answers is a challenge. The following will help.

What Information Exists?

An organization cannot get control of information it doesn't know it has. Data is everywhere, and it is growing exponentially. *Big data*, which comprises large collections of data sets that are difficult to process using traditional data processing applications, presents an added challenge. These collections are often pulled from a wide variety of sources and analyzed to create new information, which means all the data points must be known and understood to correctly answer the "What?" question.

Where Is Information Stored?

Where are the software systems being used, and where is the hardware that is storing the information? Is information at an offsite warehouse or other storage facility? Is information in the cloud? If so, where is the cloud's physical hardware being maintained? The organization should have a data map that answers these questions, showing what information it has and where it is.

Who 'Owns' the Data?

Contrary to what many might answer, IT does not own the organization's information; IT is accountable for maintaining the operating systems. To determine ownership, you must know which business unit is the primary user of each of the organization's systems. In addition, you must know who should have access to the information and at what level, as well as who can create and who can modify it.

It's not all about the data. You also must identify who can create and modify information structures, such as shared drives or SharePoint. For example, for each information structure, you must identify and document:

- Who owns the budget for the system
- Who determines and controls access rights
- Who can delete information
- Who is restricted to just viewing information
- The policies for protecting the data in various situations, such as when an employee is terminated

If an owner is not identified and the budget for the system is cut, the system and the information in it may simply disappear or be orphaned.

Why Is Information Retained?

All information should be governed by a retention policy. Obviously, if information is being used, has business value, or has legal/regulatory requirements to keep it, it needs to be retained. To determine whether these criteria apply, you must know how old information is, as well as when, by whom, and for what purpose it was last accessed.

For example, if information was last accessed to be used as a template five years ago by an employee who is no longer at the company, is not needed for business purposes, and is no longer required to be kept for legal or regulatory purposes, it may not need to be retained.

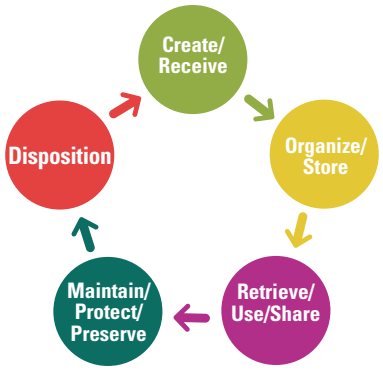
However, before disposing of it, you also must determine whether it is subject to a legal hold – and who has the right answers to this question and the previous ones.

When Can Information Be Disposed?

Before information can be disposed of, you must know whether it has met its retention requirements shown in the retention policy and whom to contact for disposition approval.

You also must have documented compliance procedures to support the expeditious review and approval of expired records to ensure their timely disposition.

ILM Defined



How Is Information Stored?

You must document how information is stored and maintained and whether it is protected, both from a business continuity and a security perspective. Determine:

- If information is regularly backed up
- Where backups are held and on what media
- How often backup media is rotated
- How often backup media is tested to ensure its data can be restored
- If backup procedures have been audited to ensure compliance
- How destruction of expired data (especially confidential content) is handled

A business continuity plan must be integrated into ILM policies and procedures. For example, if backups are stored near the office, they may be threatened by a local disaster. If thousands of miles away, they may be difficult to access.

Consider Third-Party Services

Today, most organizations outsource a variety of operations, such as security, benefits administration,

ILM Benefits

- Increased Availability
- Reduced Risks
- Reduced Costs
- Increased Business Efficiencies

and IT, and/or they engage with outside experts, such as law firms, engineering companies, accounting firms, and consulting companies. The what, where, who, why, when, and how questions need to be answered for all third parties that are responsible for the organization's information during any part of its life cycle.

This means that language that obligates third parties to follow the organization's information policies and procedures must be included in their contracts. For example, a contract with a cloud vendor must be scrutinized to determine if it complies with the organization's document management and retention policies. In addition, third-party compliance should be audited.

Step 2:
Get Executive Support

We all know "everything rolls downhill," which usually carries a negative connotation. In the case of ILM, this is a positive! The directive to manage information must come from "above" – the executive level – if employees are expected to comply.

Just as the human spine supports the entire body, the C-level is the backbone that supports this initiative's success by:

- Validating that the program aligns with organizational goals
- Communicating the business value of compliance
- Defining roles and responsibilities
- Delegating and enforcing accountability
- Demonstrating its own compliance

Step 3:
Establish Partnerships

Establishing partnerships with others in the organization provides great value, including the benefit of synergy. In the case of implementing ILM, partnerships should include, at the very least, members from legal and IT. It also may be of value to include key members from other areas, such as risk, compliance, internal audit, and some business units. Their perspectives can lead to a more strategic approach, and getting their support will help build momentum for a successful program.

Step 4:
Form a RIM/IG Committee

The RIM/IG Committee should include not just members from the executive level and from the partners mentioned above, but also people who understand how their business units use information to achieve organizational goals. Choose those who are long-term employees, familiar with the organization's culture and processes, and considered the "go-to" leaders for business initiatives.

This committee can also be the catalyst for ensuring that change management and continuous improvement processes represent the organization's dynamic needs.

Step 5:
Establish Policies and Procedures

Develop clear policies and procedures, provide employee training at orientation and regularly thereafter, make their documentation easily accessible, and ensure that employees know where to get guidance about them so that expectations for compliance and the consequences for noncompliance are clear.

These policies should take into account the organization's culture, such as its tolerance for risk. For example, will some want to keep information "just in case" rather than comply with the retention policy?

Because organizations are dynamic and laws/regulations change, policies and procedures should be reviewed annually, updated as needed, and communicated to all employees, utilizing the C-level and the RIM/IG Committee for support.

Step 6:
Provide Guidance for New Systems

The business units that are usually included when considering new software systems are those requesting the system, procurement, IT, and legal. Make sure you are also involved to ensure that new systems comply with all relevant ILM policies and regulations and that data in the new system can be purged in compliance with the retention policy. When new systems are implemented is also the right time to update the data map.

Step 7:
Monitor All Systems

You must work with whomever "owns" the system, including whomever owns its budget, to help ensure that its data is classified properly so it will be maintained in compliance with retention policies.

Working with whomever has the authority to authorize the final disposition for information ensures that it will be managed appropriately through this last step in its life cycle.

Step 8:
Document Due Diligence

Document these steps, including the development processes, because this demonstrates that due diligence was taken in establishing the ILM approach. Such evidence may be needed if ever the courts question the organization's motives for how it manages its information.

To ensure that the corporate

knowledge of information systems remains current and accurate, review and update this documentation at least annually.

ILM as Foundation

Although ILM has been practiced by RIM professionals for more than three decades and has its basis in managing paper and other physical information, it is even more essential today given the tremendous growth of electronic information.

In fact, ILM is foundational to information governance, which provides the structured framework and accountabilities that allow an organization to leverage its information assets to achieve its business goals. Ensuring that your organization is managing its information throughout its life cycle in compliance with all policies and procedures is fundamental to an effective IG program. **END**

Melissa G. Dederer, IGP, CRM, can be contacted at Melissa.Dederer@ironmountain.com. *April Dmytrenko, CRM, FAI, can be contacted at* ADmytrenko2@aol.com. *See their bios on page 47.*