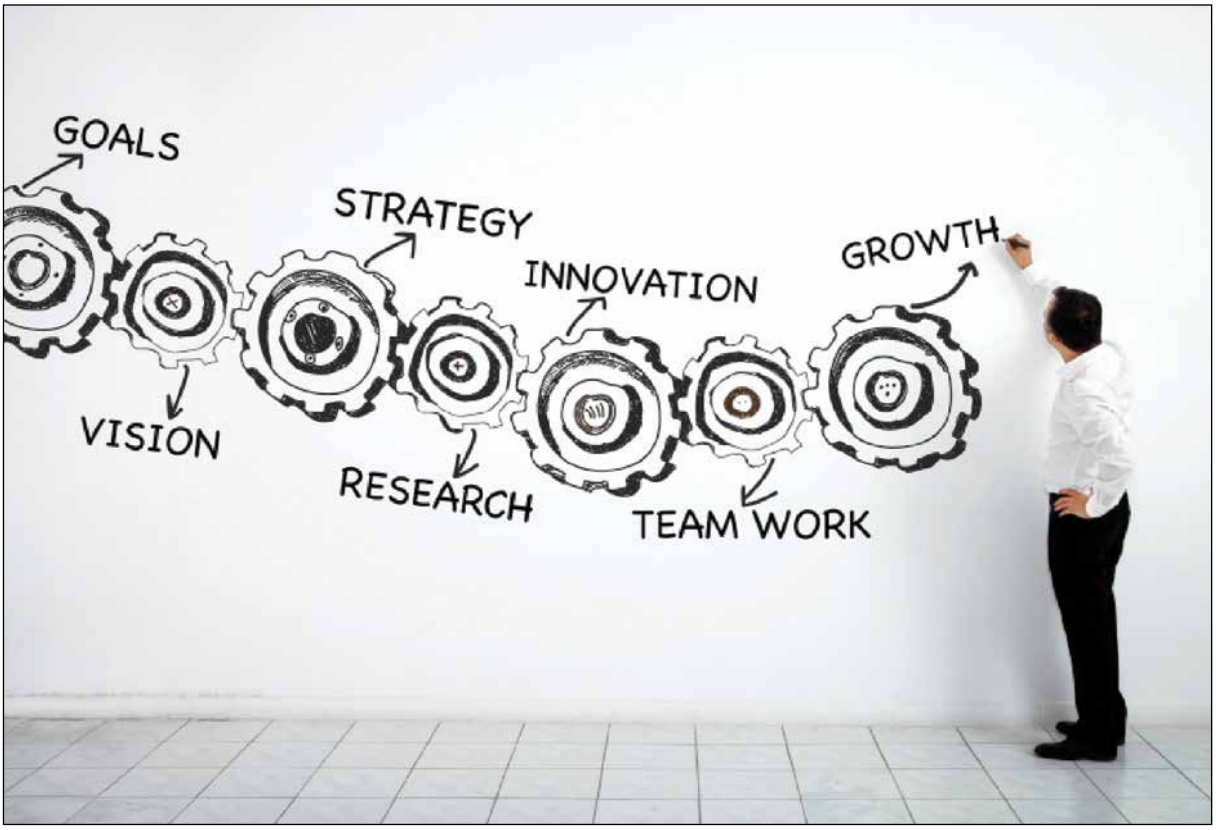

How to Develop and Implement an Effective RIM Policy

Blake E. Richardson, CRM, CIP

Business policies provide an organizational framework in which employees are expected to operate. Effective policies provide clear directions and expectations, enhancing consistency and eliminating employee "guess-work" factor. Policies should cover a multitude of topics, from business ethics to sexual harassment to travel and entertainment and, yes, records and information management (RIM).

Of course, not all policies are created equally. While some policies leave the employee with a clear understanding of what to do, others are ambiguous, leading to misinterpretation and inconsistent behavior. It is difficult to govern behavior with policies employees cannot understand. So, keep the language simple. Avoid verbosity, acronyms, and complex sentences. Policy writers must also keep in mind that they know the subject matter much better than most readers do.

It is important to note that a policy should communicate to employees *what* to do, not *how* to do it. The policy message can quickly become lost when individual procedural steps are incorporated. Employees are left to separate *what* they should do from *how* to do it. However, it is appropriate in a policy document to say that procedures related to a policy exist and where they are.

Policies communicate specific guidance and expectations that they will be complied with – both internally and externally. But, employees must have the necessary resources to comply; a policy must not set up employees for failure.

Basic Policy Components

The following sections describe basic policy components that should be included.

Purpose

A policy should begin by stating its purpose and what it addresses. Here is one example of describing the purpose of a RIM policy:

This policy is intended to assist all employees in effectively managing the organization's records and information. It will help ensure that all records and information necessary for fulfilling operational, legal, regulatory, and tax responsibilities are readily accessible and retained for the appropriate period and properly disposed of when their retention period has expired and they have been approved for destruction or deletion.

Scope

A policy scope summarizes the policy and identifies whom it applies to. For example, "This policy applies to all company and temporary employees as well as contractors, and it governs the management of physical and electronic information."

Glossary

Because a policy often includes terminology that some employees might not know, always include a glossary. Electronically posted policies often contain hyperlinks to each definition.

Audits

Inform all parties included in the scope that policy compliance is subject to internal and external audit.

Basic RIM Components

After establishing basic policy components, focus on RIM-specific topics that will help ensure that organizational content is managed in an efficient and compliant manner. Following are common RIM policy components.

Vital Records

Include a section on identifying and protecting vital records. For example, the policy might state, "It is the responsibility of the department heads to identify their operation's vital records." In addition, the glossary should define the term to educate employees on what constitutes a vital record.

Because a policy often includes terminology that some employees might not know, always include a glossary. Electronically posted policies often contain hyperlinks to each definition.

Retention Schedule

The RIM policy should address the purpose of the retention schedule, how to read it, and the need to comply with it. The policy should provide guidance on how to update the schedule.

Legal Holds

This section of the policy must provide specific direction on employees' responsibilities for handling legal holds. Policy language might say, "Any information on hold because of an active or anticipated lawsuit, audit, or regulatory inquiry must be retained even if its retention period, according to the organization's retention schedule, has expired."

Record Storage

The policy should say that company records are to be stored only with RIM-approved vendors and that individual departments cannot enter into contractual relationships with storage vendors.

Hard Drives and File Shares

A RIM policy should guide employees on the appropriate use and maintenance of hard drives and file shares. For example, "Local hard (C: drives) are not to be used for the storage of company records or content of business value. This type of information must be stored in a repository accessible by employees with appropriate authorization." The policy should also communicate that employees must maintain the content they save to hard drives and file shares.

E-mail

How an organization manages e-mail is primarily dependent on available technology. Therefore, it is important to understand what capabilities exist, such as e-mail management and archiving applications, Outlook personal storage table (more commonly referred to as .pst) folders, and enterprise content management software. The RIM policy should provide direction to employees in accordance with available technology.

Regardless of existing technology, basic e-mail policy components need to address such topics as forwarding business e-mails to personal e-mail accounts, minimizing the distribution of attachments, and evaluating e-mail content for retention purposes.

Information Destruction/ Deletion

Include a section that addresses the proper methods for the de-

… it is imperative to collaborate with each department during the policy draft phase and to have those departments conduct a final review before the policy is distributed.

struction and deletion of physical and electronic information, advising employees that only vendors approved by the RIM department are to be used.

Additional Policy Considerations

As technology advances, RIM policies need to keep pace. The following topics are being incorporated in many RIM policies.

Social Media

Many organizations have issued general-use social media policies with a focus on limiting what an employee can post. Because organizations want to preserve their image and prevent the disclosure of proprietary information, their social media policies might state that employees are prohibited from posting disparaging comments about their employer. In the United States, though, a policy that prohibits employees from posting about their wages or working conditions might conflict with Section 7 of the National Labor Relations Act, which allows non-management personnel to do just that.

A RIM policy should approach social media based on content. If posts submitted by employees as part of their job function or posts received on the organization's social media sites from the public constitute an organizational record, then the content should be retained in accordance with the retention schedule. In addition, the organization must have the ability to preserve social media content (created and received) in the event of litigation or regulatory inquiry.

Cloud

Cloud storage and computing can reduce capital expenses related to data center hardware, software, storage, supplies, and maintenance. Before bouncing to the cloud, though, RIM professionals should ensure the RIM policy addresses the things that put the organization's records and information at risk. The policy should address requirements such as availability, security, data ownership, and retention.

Bring Your Own Device (BYOD)

The advent of personal "smart" technologies has required organizations to rethink their approach to company-only devices for accessing and processing information. Many employees question the need to carry company-issued phones and laptops when their personal devices can perform many of the same functions.

An organization should issue a BYOD policy that addresses such topics as types of devices allowed, connection protocols, and the need to sign a waiver. The RIM policy should address issues related to device security, to imaging data on the device for legal hold orders, and to separating personal from corporate information.

Getting Policy Approval

For a RIM policy to be successful, other departments must abide by it. Therefore, it is imperative to collaborate with each department during the policy draft phase and to have those departments conduct a final review before the policy is distributed. Listed below are departments and specific policy topics that require collaboration.

IT

RIM policies often require electronic records with long-term retention to be accessible for the duration of their assigned retention period. This requires IT to have a data migration strategy that ensures the operating systems and applications needed to access the information remain available.

During the draft phase, the RIM professional should confirm that IT can meet the migration requirement; together, RIM and IT can then work out the policy language. If IT does not have the capability to properly migrate data, the requirement should not be in the policy until it does have that capability.

Internal Audit

For a policy to be successful, employees must comply with it. Further, there must be ways to measure compliance. Thus, the RIM policy should tell employees that compliance will be audited.

Often the RIM department will not have the resources to audit the policy and therefore will rely on the internal audit department. In such cases, the RIM professional should collaborate with internal audit to determine what needs to be audited, what constitutes compliance, and if that group has the resources to do the auditing.

Legal

RIM policies should include language on legal hold orders that has been approved by the legal department. Often, legal departments will conduct a full review to ensure a policy does not violate labor practices or laws.

Distributing the RIM Policy

After the RIM policy has been approved, determine the most effective method for distribution.

Distributing hard copies is the least recommended option. Because policies are periodically updated, employees might keep several versions and are therefore more likely to refer to outdated versions.

E-mail attachments are preferable to a hard-copy release, but they include the same risk: employees might electronically file the soft copy and subsequently refer to it even after the policy has been updated. E-mail attachments can include a request for employees to respond to the message, acknowledging their receipt of the policy.

The best method is to send an e-mail containing an intranet link to the policy. Some organizations use a database to track which employees have accessed the policy. When using database tracking, design the policy form to include an e-acknowledgement – a box the employee clicks to acknowledge receipt and review of the policy.

Auditing for Compliance

For a policy to be successful and credible, it must be enforceable and its compliance measureable. Organizational policies are frequently the focus of lawsuits and regulatory inquiries. Therefore, organizations should be able to provide evidence of establishing relevant policies, training employees to follow them, and auditing for employee compliance with them.

Audits also can provide insight into a policy's effectiveness. The results might indicate negative trends that can be analyzed and resolved.

The following elements should be included in an audit plan:

Audit Areas

Determine what policy components need to audited. Include areas that create the greatest potential for risks from non-compliance.

Testing

After identifying elements of the policy that need to be audited, establish a process that allows the auditor to accurately test for compliance.

Communication

Distribute a communication plan to all operations subject to the audit. The plan should tell employees when the audit will occur, what will be audited, and how to prepare for it.

Audit Findings Report

After the audit, the auditor must send a report of the findings to management. The report should communicate areas of non-compliance, the degree of organizational risks, and recommendations for resolving the issues.

Conclusion

An effective policy is fundamental to the success and credibility of a RIM program. Therefore, it is important to develop a RIM policy that is easy to understand, encompasses key components of the program, and provides employees with the guidance they need to ensure organizational content is managed in an efficient and compliant manner. **END**

Blake Richardson, CRM, CIP, can be contacted at titansfan100@gmail.com. *See his bio on page 47.*