IRON MOUNTAIN®

RECORDS AND INFORMATION MANAGEMENT

BEST PRACTICES

A Practical Approach to Building a Comprehensive and Compliant RIM Program

INFORMATION IS...**YOUR ADVANTAGE**

Contents

Why Do You Need Best Practices for RIM?

While we live in the Information Age, not all information created or received by an organization rises to the level of being an official business record – this important subset requires deliberate management because these records provide evidence of business transactions, decisions and satisfaction of legal obligations. Management of records has become increasingly complicated due to the wide array of formats we work with: paper, electronic files, email, instant messages, social media, big data and more. It is further challenged by where those records can be found: in numerous applications, SharePoint®, file shares, mobile devices, the cloud, tape and the list goes on. In addition, industry- and segment-specific regulations around records management continue to expand. A compliant Records and Information Management (RIM) program is necessary for organizations to proactively and progressively manage all business record content, regardless of its format or location. Organizations need to demonstrate "good faith" intentions to follow these best practices consistently and accurately, with audits playing a vital role for defensibility.

As the number of laws and severity of punishment related to governing records continue to increase, it is becoming paramount that organizations implement and execute the best practices for proper records and information management.

IRON MOUNTAIN®

The Iron Mountain best practices initiative is a direct response to requests from our customers for guidance on:

- Best-in-class compliant RIM practices
- Continual program improvement ideas
- Government regulations that impact RIM

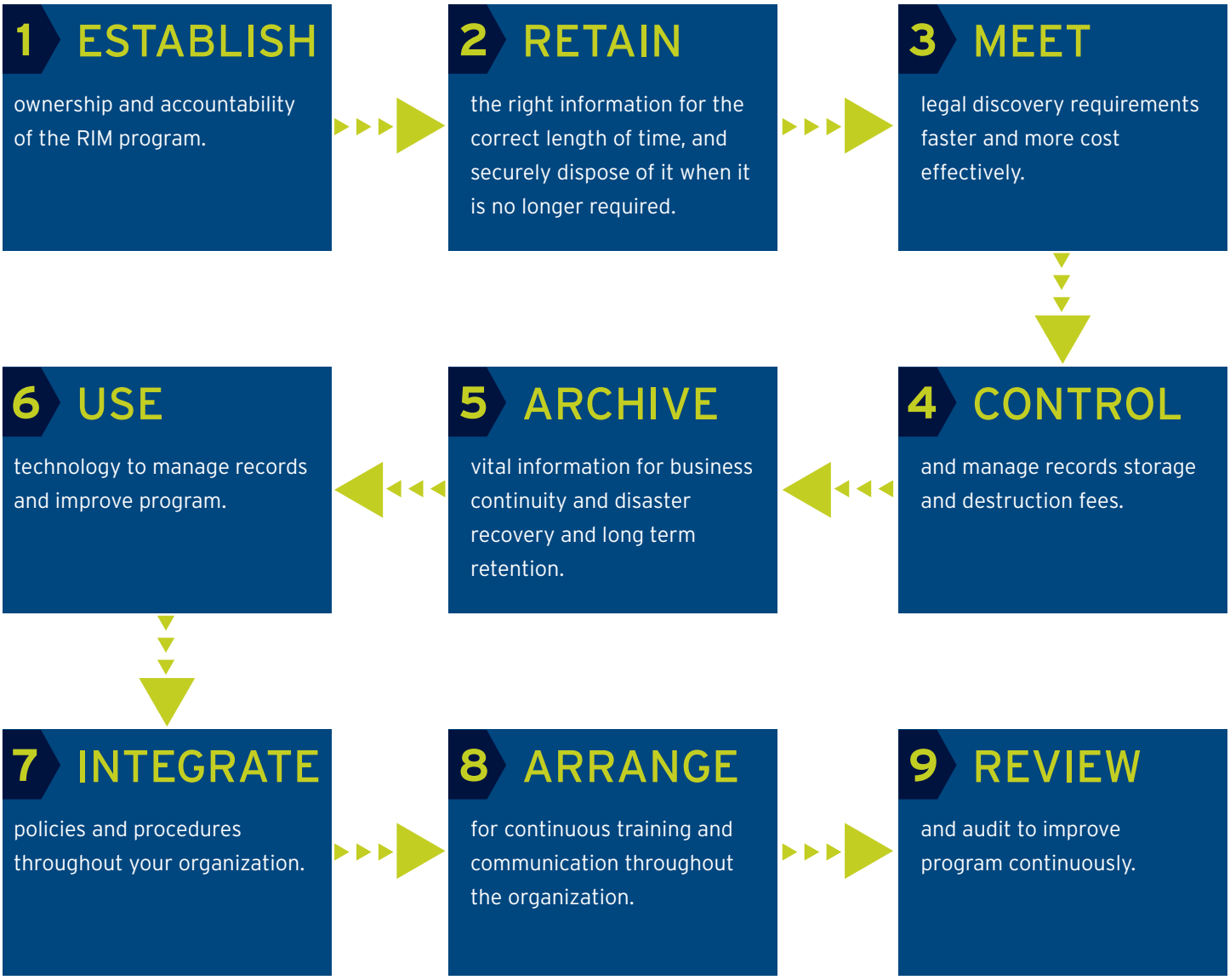
Now, more than ever, it is critical that organizations have solid records management practices in place for all record types, across all business units and in all countries. These practices should feed into a comprehensive and consistently applied RIM master plan. Organizations that meet and demonstrate regulatory compliance will successfully mitigate litigation risk, while others scramble to protect their corporate reputation and shareholder value.

This RIM Best Practices guide represents the collective experiences of hundreds of thousands of Iron Mountain customers – and more than 60 years of records management history. From those years of experience, records management fundamentals have been tried and proven true, processes and workflows have been crystallized for greater efficiencies and less exposure, and best practices have evolved to cover the many integral aspects of proper records management, including the explosion of electronic records. These best practices are provided here as a practical approach to a comprehensive and compliant records and information management program.

HARRY E. EBBIGHAUSEN
President, North America, Iron Mountain

Key Components
of Information Governance

Information Governance is the multi-disciplinary enterprise accountability framework that ensures the appropriate behavior in the valuation of information and the definition of the roles, policies, processes, and metrics required to manage the information lifecycle, including defensible disposition. An organization with a solid foundation of proven successful RIM practices will foster collaboration among key stakeholders in an environment of comprehensive information governance: legal, IT, business units, records management, compliance etc. It will also:



These components are integral to a compliant RIM program. Independently, each represents a good practice. As a unit, they serve as a solid foundation of best practices for RIM. They also align with the Generally Accepted Recordkeeping Principles® put forth by ARMA® International to foster general awareness of information governance standards and principles and to assist organizations in developing information management systems that comply with them.[1]

[1] http://www.arma.org/garp

WHY IS CONSISTENCY SO IMPORTANT?

There is one phrase that resonates as a theme for simple and complex aspects of compliant records and information management programs: CONSISTENCY IS KEY.

Records Managers are being advised by judges involved in discovery cases to destroy records that have met their retention requirement, provided they are not on a legal hold and that there is an approved Records Retention Schedule in place.

Steps for consistency begin with developing an enterprise-wide Records Retention schedule for your organization and implementing it across all business units and countries. Writing, publicizing and training employees about your RIM Policy and Procedures will assist with making it a standard in your organization. Instituting a records coordinator network in the business units or departments will enable compliance. Formalizing records destruction practices for both paper and electronic records, and destroying records consistently and systematically with the help of technology are important as well. Regularly auditing your program and remediating for inconsistent practice is vital to keeping your system working to its most efficient degree.

RIM BEST PRACTICES

1. ACCOUNTABILITY
2. RETENTION
3. POLICY AND PROCEDURES
4. IMAGING
5. ARCHIVAL TAPE MANAGEMENT
6. COMPLIANCE
7. DISPOSAL

These and many other aspects of Compliant Records Management are listed after each of the seven Best Practices areas. Keep your program elements simple: perfection is the enemy of "good" and remember that your program can evolve over time. Your RIM program will be judged by the consistency of its implementation and execution, not the details of the program's design. For each of these Best Practices areas we have included an overview and tips for compliance.

ACCOUNTABILITY

WHERE DO WE START?

Awareness of RIM is required at every level of the organization to achieve compliance. Without senior-level sponsorship and commitment, the program is far less likely to thrive. There should be a corporate records manager to administer the program for the enterprise, as well as a designee in each business unit accountable for implementation in their area. Finally, each employee should be required to acknowledge that they have read and understood the RIM policies and procedures.

Ideally, a Senior Executive should be named as the owner or advocate of the program. This person typically sits in the Legal, IT, Compliance or Risk functional areas. He or she should be able to help influence practices, personnel and funding necessary to ensure compliance.

The early creation of a steering or governance committee composed of senior management across key departments is instrumental to the success and implementation of a compliant RIM program. By creating an active steering committee, your organization will be positioned to proactively address the changing business climate and the ever-increasing regulatory controls for RIM. And, we have learned that successful and sustained programs require top-down leadership.

Once your steering committee members have been identified, we suggest they each read and make sure they fully understand the best practices in this guide.

1 ESTABLISH

an enterprise-wide RIM program Steering Committee consisting of eight to ten people, composed of a designated records manager and representation from legal, IT, compliance, tax, human resources, risk management and key business units to be responsible for oversight of the RIM program, high-level management and strategic insight.

2 SCHEDULE

Steering Committee meetings at appropriate intervals to assess the current state of the RIM program. Specific responsibilities include providing high-level management and oversight of the program, and ensuring that the RIM program is properly maintained and adhered to, and updated by recommending/approving staff and system resources.

3 DESIGNATE

a Corporate Records Manager to administer the program and facilitate accountability throughout the entire organization.

4 SUPPORT

the records management function with the appropriate resources and experts, both internal and external, by providing online RIM training for all employees, testing for certification and engaging the business units in the process early and often, as they are ultimately responsible for making compliance happen.

5 COMMUNICATE

RIM program information regularly to employees through engagement with internal marketing and communications resources.

RETENTION

At the heart of a legally compliant records management program is the Records Retention Schedule. This policy tells you how long records need to be kept - and when you can dispose of them. This is the platform for protection of organizational assets as well as the surest method to avoid risk and litigation and to control program costs.

The Records Retention Schedule informs an organization how long records must be kept for legal, regulatory and operational requirements. Compliance with the Schedule protects records during their useful life and if done in a systematic and controlled manner, enables their defensible destruction.

A Records Retention Schedule supports an organization's efforts to:

- Meet regulatory requirements
- Manage intellectual property
- Control the costs of information storage
- Locate and retrieve documents for legal discovery
- Dispose of records at the end of their business life

The Records Retention Schedule represents all records in all formats created by an organization across all countries, divisions and functions. Retention periods are based on jurisdictional federal, state and province legal and regulatory requirements, along with operational overrides.

The development of a legally credible Records Retention Schedule is broken down into four activities:

A. Profile your business related to risk and functions performed in each country

B. Create a universal classification scheme

C. Perform legal research

D. Overlay operational retention requirements

A. PROFILE YOUR BUSINESS

It is important to understand the business your organization conducts in all your locations. Knowing where an organization is most frequently litigated, investigated or audited is valuable in assessing risk and assigning resources appropriately. With increasing frequency, your customers are requesting audits of records related to them within your organization, so it is necessary to know where those records exist and the kinds of controls that are in place for their protection.

B. CREATE AN ENTERPRISE-WIDE RECORD CLASSIFICATION SCHEME

One of the most important tasks in organizing your records is to establish a records classification scheme. A record classification scheme is a grouping of records by the business function, record class and record type that is used to create the Records Retention Schedule. Your class scheme can be developed in a number of ways. The easiest is to work with a trusted third-party who can provide a template of the kinds of records (both paper and electronic) that you expect to find within your industry. These templates can then be edited to conform to your individual business. Third-party experts also bring vast knowledge about macro-RIM trends and requirements, as well as industry-specific regulations.

Alternatively, you can inventory the records yourself and organize them in the best practices hierarchy as follows:

The highest level of the classification scheme hierarchy is a business function. Functions are the primary work areas of your business and include common groups such as human resources, tax, accounting and legal as well as those that are unique to your particular business such as research and development, claims, manufacturing and funds management. Most organizations will have around 20 to 25 functions. (Note that these are not departments. Functions are used to protect against organizational changes.) Within functions are groups of records that support a common work process called record classes or series and are composed of record type examples. The best practice trend is to create larger buckets of records – and therefore fewer classes with greater distinction between them – to make it easier for users and/or tools to classify records.

Also, each class should have a unique identifier to facilitate indexing and access. The following is an example:

Classification Code: ACC1000

Record Function: Accounting

Record Class: Accounts Payable and Receivable

Record Types: Accounts Payable Aging Reports, Accounts Payable Distribution Reports, Cash Disbursement Reports, Accounts Receivable Reconciliations, Accounts Receivable ACH and Wire Data

C. PERFORM LEGAL RESEARCH

It is important to conduct legal research to determine the retention period for each record class. This work requires the assistance of legal counsel, consultants, external RIM experts or licensed access to a provider of citations. At a minimum, federal and state types of legal requirements must be considered for each country.

You must review and take into consideration the statutes of limitation and limitation of actions that dictate the period of time in which a lawsuit may be filed or a fine assessed when establishing a final retention period for the organization's records.

You will also need to define for each record class, the triggering event (such as a business acquisition, merger or employee separation) that must occur for a record to become inactive, thus signaling the beginning of the retention period countdown.

D. OVERLAY OPERATIONAL RETENTION REQUIREMENTS

In addition to legal requirements, operational retention requirements of your business must also be taken into account. On occasion, records may need to be kept longer than their legal requirement to support your operational needs (for example: retaining "big data" to track marketing trends.) These requests should be the exception rather than the rule. The final approved retention period for the record class is the longer of the legal and operational rule.

Examples of groups that issue such regulations include:

- U.S. Securities Exchange Commission (SEC)
- Federal Trade Commission (FTC)
- Federal Communications Commission (FCC)
- Environmental Protection Agency (EPA)
- National Labor Relations Board (NLRB)
- Internal Revenue Service (IRS)
- Equal Employment Opportunity Commission (EEOC)
- Occupational Safety and Health Administration (OSHA)

1 DEVELOP

and implement a single enterprise-wide Records Retention Schedule for all business units that captures all the records, regardless of format, created or received by the organization in the conduct of business.

2 PRESERVE

records with long term retention requirements in media-appropriate archival conditions.

3 REEXAMINE

the Records Retention Schedule for updates and revisions at least every two years to ensure that the classification scheme and legal research are current.

4 DESIGNATE

business records, by way of policy, as either "official" or "unofficial" (convenience copies, versions). The Records Retention Schedule governs the retention period for the "official" records. "Unofficial" records are typically retained until no longer needed but never longer than the official record.

5 REDUCE

the number of records that have no ongoing business value or usefulness in order to reduce risk and cost. Conduct corporate-wide annual reviews of onsite records to determine those that are no longer active. Inactive records may be sent to offsite storage or placed in a designated archive. And records, paper and electronic, that have met their retention requirement can be disposed of.

6 IDENTIFY

vital or "mission critical" records that are essential to the financial, legal and operational functions of the organization and its customers, employees and shareholders.

7 ESTABLISH

a process to implement the Records Retention Schedule to include initial and ongoing training programs for all employees within the organization.

TO FACILITATE THE MANAGEMENT OF EMAIL:

- Create an "E-Schedule" subset of the Records Retention Schedule that shrinks and consolidates the available email record classes. This "E-Schedule" simplifies the email classification and archiving process for employees and/or tools.
- Put in place an email policy that explains to employees how to classify and retain emails that are official records as well as the deletion of non-record email.
- Prohibit the use of PST and NSF files to reduce risk.

OTHER RECORD FORMATS:

Keep in mind that records can be created by way of websites, blog posts, instant messages, wikis, Twitter, Facebook and other communication platforms. We cannot avoid these new and dynamic vehicles for enhancing business, but we must be aware if records are created within them, and if so, how they will be captured, retained and destroyed per the Records Retention Schedule.

POLICY AND PROCEDURE

An organization's RIM program should be supported by an enterprise-wide policy and associated procedures that address each component of the RIM program in accordance with operational and legal requirements. The overarching RIM policy should be relatively short (four to six pages) and address records ownership, roles and responsibilities, the records lifecycle, legal holds, training, maintenance, audits and version control. While there may be separate procedures for records retention, active file management, inactive file management, vital records, email management, social media, use of the cloud and any other area of RIM, they should conform to the expectations set in the policy. The policy and procedures should be accessible and communicated clearly and consistently throughout the organization, ideally in a dedicated intranet site or collaborative workspace.

1 CREATE

a policy and procedures that are not a "wish list" but for which compliance is achievable while meeting legal and operational requirements.

2 INCORPORATE

all media types and formats, including social media, email and instant messaging.

3 REFER

to other information governance policies as applicable.

4 DEFINE

and outline the handling of official versus unofficial records and active versus inactive records.

5 ESTABLISH

a system of record for centralized management of your RIM program. Fewer systems offer greater control.

6 ALIGN

- back-up policies with email retention policy.
- automatic purge policy with discovery policy.

7 ESTABLISH

procedures for systematic records destruction such as annual organized purges of records to identify and either send them to offsite storage or to delete or destroy. This prohibits selective destruction of records.

8 ASSIGN

a system to hold records subject to litigation, audit or governmental investigation either in process or being commenced at some point in the future. Records that are under a "hold" order should not be destroyed even if they are eligible per the organization's Records Retention Schedule.

9 DEFINE

the RIM-related roles and responsibilities within an organization including those for the Steering Committee and create a position that will be responsible for overall RIM administration.

10 INSTITUTE

storage procedures for onsite, offsite and electronic records.

11 IDENTIFY

and protect vital records for the continued operation of an organization in the event of a disaster.

12 WORK

- with IT to establish business continuity and disaster recovery procedures.
- with IT and Legal to create policies for use of social media, employee-owned devices, the cloud and other emerging tools.
- with IT and Legal to create a corporate-wide email management policy.
- with business units to understand the value and management of their records.

YOUR EMAIL MANAGEMENT POLICY SHOULD INCLUDE SUCH COMPONENTS AS:

- A clear statement that email content belongs to the company.
- Defined limitations on personal use of email, communicate that there is no privacy of corporate email.
- Clear definitions of what is and is not appropriate email content.
- Password and encryption standards for the company.
- Employee sign-off that they have read and understood the policy.

IMAGING

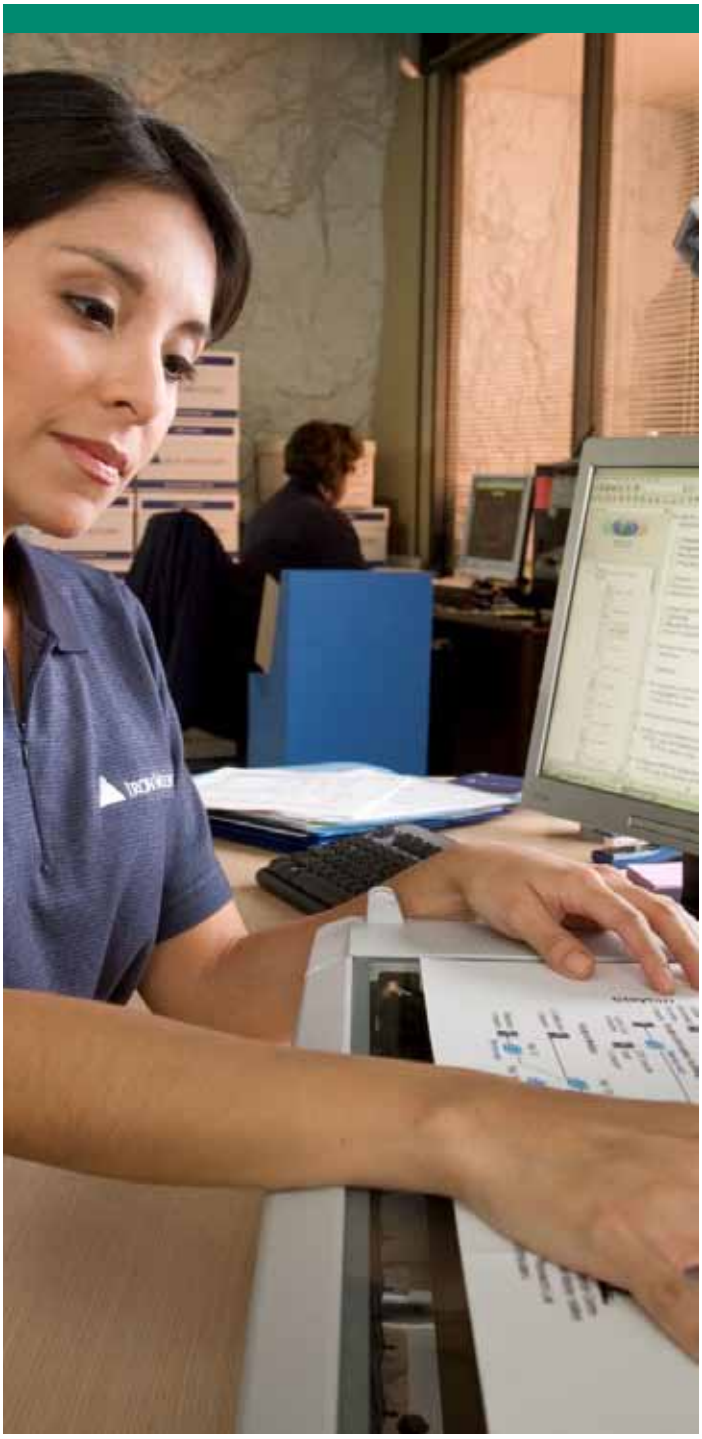
In the private sector, as many as 95 percent of official records are in an electronic format, whether they are created within an application or are scanned to create a digital image – and the public sector is rapidly catching up. Organizations with paper in their workflows need to consider if scanning the paper will improve the efficiency of the process, accessibility by approved employees or customers, and overall management of the content in compliance with their RIM policy. They then must determine if the cost of imaging aligns with the proposed improvement to the business process.

The same consideration should be given to legacy paper records. For most organizations, it does not make sense to convert all legacy paper records to digital images. Based on business need, organizations may opt to image entire cartons of records or selectively image "on demand."

It is important for an organization to determine what happens to the paper records after they have been scanned. Business areas that intend to destroy original records should seek the guidance of the Legal department. If an area decides to use electronic records as the official version of a record, they then take on the burden of defending the process and system.

In the United States, reproductions produced by any technology (including electronic imaging) are considered to be legal for all purposes, including evidence and regulatory compliance. Since both the reproduction and the original have the same legal status, the originals can be destroyed after reproduction since there is no obligation to keep two versions of the same record. There are, however, notable exceptions such as wills, codicils, promissory notes, broker trading cards and real estate deeds.

If the electronic version of a record is declared as the official record, then the systematic destruction of the original should occur to minimize storage cost and risks related to discovery. Careful examination is necessary before blanket destruction of your paper takes place.



1 ACCURACY AND ACCESSIBILITY

The quality of the digital image must be accurate (both sides are scanned, the image is legible, etc.). The scanned image file should be indexed using appropriate metadata and stored in a system that can be accessed by authorized parties.

2 DESTRUCTION OF ORIGINALS

Departments intending to destroy original records should seek the guidance of the Legal department. If a department decides to use electronic records as the official version of a record, they then take on the burden of defending the process and system.

3 COST EFFECTIVENESS

Scanning records and storing records as digital images may be more costly than retaining them in paper form. The added costs of digital imaging can be justified when their access and retrieval must be fast, workflow processes can be optimized in conjunction with imaging paper inputs, paper records are too cumbersome for everyday use, or the paper records need to be utilized by multiple workers who may be in multiple different locations. In such cases, the originals may be scanned and sent to secure storage, while the images are used as the "working" copies.

4 COMPATIBILITY

Departments planning to implement digital imaging are advised to seek the advice of the Information Systems department to ensure that the proposed system is compatible and consistent with the company's overall technology strategy.

5 PERSONAL INFORMATION PROTECTION

Departments planning to implement digital imaging must seek the advice of the Legal and Information Systems departments to ensure that the proposed system has adequate controls in place to secure the system from third-party interference and protect personally identifiable information in compliance with the company's confidentiality policy.

6 APPLICATION OF THE RECORDS RETENTION SCHEDULE

All content repositories that house electronic images of records must comply with the requirements of the Records Retention Policy. Such systems must be configured to support the retention and deletion of images/records in compliance with the Records Retention Schedule.

7 LITIGATION HOLD CAPABILITY

When records are placed on "hold" as a result of litigation, audit, or regulatory investigation, content repositories that house electronic images of records should accommodate the identification, flagging, and preservation of the affected records for the duration of the hold order.

ARCHIVAL TAPE MANAGEMENT

The success of a RIM program hinges on the ability to access information for business support, litigation response, compliance and audit and eventual destruction. Organizations need the ability to access records by multiple indices or metadata such as a unique Records Retention Classification code, subject matter (content and context), record creator, intended recipient, date, data security classification, etc. Proper indexing methods are one of the easiest ways to recognize significant returns on investment.

Well-indexed records ensure easy access, reduced retrieval time and financial cost. Poor indexing methods will result in additional litigation fees and increased labor cost. The inability to satisfy record retrieval or disposition requirements can result in major fines, increased litigation, unnecessary storage costs and the degradation of overall service quality within an organization.

Access and indexing are dependent on one another because records must be properly organized to enable timely, accurate and controlled access. Just as an index in a book directs the reader to a specific page, a records index directs the record user to a particular place where the required information is located. The location may be a carton, file folder or an electronic storage location, such as a network directory, email archive, SharePoint®, or Electronic Document and RIM (EDRM) system. Once the record location is identified, access can be authorized by various security controls.

An increasingly important use of metadata or indices is to help manage the most effective, cost-efficient storage of records throughout their lifecycle. Knowing the class of record, its retention requirement and age and its security designation will support the decision to move the content to lower-priced storage options, such as an offsite physical locations, the cloud, or onto tape that allows for indexed information about records or data to be retained.

Just as organizations must classify and index records going forward, you must also consider the "clean-up" of legacy records, both physical and electronic. Tools exist to help associate metadata, and actual content in the case of electronic records, with your Records Retention Schedule to enable destruction eligibility decisions.

1 DETERMINE

relevant indices or metadata for your business, including the Records Class Code from the Retention Schedule.

2 INDEX

all records in a systematic manner regardless of the storage medium or location using mandatory fields whenever possible.

3 UNIFY

paper and electronic records into a single system of record to facilitate access and management.

4 FILE

paper records in filing systems and electronic records in network directories that are categorized by the same record classification scheme and time period.

5 IMPLEMENT

a proper authorization process to ensure protection of the confidentiality of an organization's records, maintain the confidentiality of personally identifiable information, and prevent unauthorized disclosure to third parties.

6 LIMIT

individual employee access to records unless it is necessary in order to conduct authorized business and is approved in accordance with established organizational practices and procedures.

7 CONDUCT

an annual formal review of the RIM system, record classification scheme and centralized index to validate that structure is consistent, accurate and appropriate and reflects any changes in business.

8 DETERMINE

the suitable turnaround time for retrieval of different categories of records from onsite or offsite paper storage facilities, and for electronic records storage such as tape or a data warehouse.

9 ENSURE

that storage of records both onsite and offsite guarantees security, consistency, accessibility and confidentiality.

10 MIGRATE

electronic records to a digital archive that can provide secure access to, and RIM functionality for, emails, instant messages and other communication formats (tweets on Twitter®, Facebook® posts) for regulatory, legal or operational purposes.

COMPLIANCE

To keep RIM front of mind, the RIM department should create a brand for itself and continue to communicate to employees through periodic newsletters, video or webcasts, posters, and other approved methods of corporate communication. Electronic learning courses should be considered to share a consistent message about your RIM program with all employees, new or long-term, near or far. Once the program is implemented it needs constant guidance and nurturing, which can be facilitated by using collaborative tools or even social media within your organization.

To ensure compliance, if at all possible, the RIM program should be integrated into the organization's internal audit process. In instances where this is not possible, the RIM department can conduct its own audit of business unit activity through surveys, questionnaires and/or interviews. A best practice is for business unit managers to attest that they understand the demands and expectations of compliance. In either case, whether conducted by Internal Audit or by the RIM department, areas of noncompliance must be noted and a remediation plan put in place.

The benefits of an investment in an enterprise RIM program will be short-lived if business units and their employees are not in compliance with the program and its policy. The critical measures of compliance are organization-wide accountability and auditing.

1 INTRODUCE

measures of performance related to consistent retention and destruction of records, both paper and electronic.

2 INCLUDE

RIM as part of the company's internal audit process to ensure that consistency, compliance and legal requirements are met wherever possible.

3 AUDIT

RIM as part of the company's Audit compliance adherence to corporate electronic records, email retention, and deletion policies by involving the IT department.

4 DEVELOP

remediation plans for areas of noncompliance.

5 CREATE

a RIM acknowledgement program that requires employees to sign a document confirming their receipt of training and understanding of RIM policies and procedures.

DISPOSAL

The systematic disposal of records is the way in which an organization can comply with regulations, minimize litigation risk and cost, and reduce storage costs. Records disposition can follow two paths: 1) the movement of the record to an authorized archive to preserve it for historical reasons, or 2) the destruction of the record once it has met its retention requirement, providing it is not on a legal hold or part of a Freedom of Information Act (FOIA) request.

Records in any format that document the organization's past, its development and significant events are considered as "archival" or "historical". Key personnel should be identified and given an official repository or format (i.e., PDF-1A) for their continued preservation and access.

Records that are not archival can be destroyed after they have met their required retention period as noted in the Records Retention Schedule. Ideally, records should be destroyed as soon as possible after they are no longer needed during periodic "clean-up" events or through systematic purges from applications or repositories based on pre-established rules. Certain types of records, particularly those that contain personally identifiable information (PII), must be destroyed as soon as they no longer have business value.

An established pattern of systematic destruction serves as evidence of an organization's good faith in attempting to conform to the law. Haphazard patterns of destruction appear suspicious and can suggest that damaging or embarrassing records were intentionally destroyed.

Records destruction should be an inherent element of an organization's overall RIM program and should cover both active and inactive records in all media. Secure methods of destruction should be determined by the RIM department working in conjunction with Legal, Compliance, and IT, and should be included in RIM policy and procedures. Upon expiration of a record's required retention period, all records identified as eligible should be approved for destruction unless there is a legitimate business reason to postpone that destruction. Any unofficial or "convenience copy" of a record must be destroyed once it has met the business need for which it was kept and should never be kept longer than the official record. For example, the official version of an expense report may be required for the completion of an organization's tax audit. However, specific departments or individuals may keep copies within their offices for convenience. Once the need for those convenience copies is complete, those versions of the record may be destroyed.

Non-confidential records may be destroyed using a variety of recycling methods.

Records that are subject to litigation, government investigation, Freedom of Information Act (FOIA) requests, or audit cannot be destroyed even when they have met their Records Retention Schedule requirement. Procedures should be in place to state that the destruction of relevant records must be suspended until such time as official notification is provided that destruction can resume. The destruction of both paper and electronic records should be documented.

The proliferation of privacy laws in certain states and in other global jurisdictions impacts the way in which organizations manage and protect records, and this includes their secure destruction. Other confidential or sensitive records such as patents and proprietary or trade secrets have security classification levels and should be destroyed in a commensurate manner, such as secure shredding and degaussing.

Non-confidential records may be destroyed using a variety of recycling methods. However, the best practice is to securely destroy all records: official or unofficial, confidential or non-confidential, and to remove the subjectivity of an employee's decision as to which is which. This is particularly relevant for highly regulated industries or certain "high-risk" functions within an organization.

A compliant RIM program must demonstrate the key elements of consistency, accountability, adoption and accessibility. These elements must be audited and updated consistently over the lifespan of the business.

1 DETERMINE

appropriate method of destruction or archiving by record class, record type or media.

2 INSTITUTE

a consistent and secure system for the destruction of records in accordance with an approved Records Retention Schedule.

3 DEVELOP

destruction procedures that demonstrate authorization, adherence to confidentiality and security requirements, and recognition of suspended records or those on "hold."

4 DISTRIBUTE

to necessary parties for their review all records pending destruction according to the organization's Records Retention Schedule and ensure that authorization for destruction is confirmed.

5 DESTROY

records securely that contain personally identifiable information about individual customers or employees. Some examples of this data include Social Security numbers, date of birth, bank account information, Personal Identification Numbers, passwords, drug prescription information, mothers' maiden names, etc. Any records that contain personally identifiable information should be classified as confidential and destroyed to protect the privacy of employees, shareholders, customers, patients and other individuals.

6 ENSURE

that employees are aware that premature destruction of records is expressly prohibited, and if intentional, may result in disciplinary action up to and including termination of employment and possible civil or criminal liability.

7 REVIEW

all official records that have fulfilled their retention period to ensure that their destruction complies with the standard policy and procedures and that the records are free of all retention holds. Give departments review deadlines from the date of receipt of the report of records eligible for destruction. Department Managers should provide justification to why specific records should not be destroyed.

8 DISCARD

any unofficial records once they have fulfilled their purpose. Under no circumstance should duplicates or drafts (unofficial records) be retained longer than the official versions of the records. When records are approved for destruction, all copies in all media and formats must also be discarded.

9 SUSPEND

all regularly scheduled destruction of relevant records (including email records) when it becomes clear that there is a possibility of litigation, audit or governmental investigation being commenced at some point in the future by or against an organization. Records that are under a "hold" order cannot be destroyed even when permitted by an organization's Records Retention Schedule.

10 REVIEW

destruction reports periodically that list records at offsite storage vendors that are eligible for destruction.

11 MAINTAIN

a final destruction listing report for paper records stored offsite that lists record identification number, destroy dates and who authorized the destruction.

12 INSTITUTE

consistent and appropriate destruction practices for records residing at both onsite and offsite locations.

IRON MOUNTAIN SERVICES

RECORDS AND INFORMATION MANAGEMENT

Iron Mountain provides compliant RIM solutions to manage and protect your information assets. Our RIM programs ensure that your business records are secure and easily accessible. We offer specialized services tailored to your unique needs.

SECURE SHREDDING

Given the confidential nature of business records, it's important to ensure complete destruction. Our secure shredding services help you to protect the privacy of your company, employees and customers.

DATA BACKUP AND RECOVERY

Whether physically transporting and vaulting your backup tapes at one of our secure facilities or backing up your data through a secure Internet connection with Electronic Vaulting, our comprehensive data protection and disaster recovery services place your information offsite, offline and out of reach; yet the data is accessible whenever and wherever you need it through proper tape management.

VITAL BUSINESS RECORDS

Our climate-controlled, secure facilities are designed to protect irreplaceable documents like original deeds, wills, trusts, contracts, patents, and other notarized and certified records for you.

CONSULTING

Today's business world demands that companies follow sound, consistently applied RIM practices. Let our consulting professionals review your current RIM program, help you determine which records you need to retain, and create an appropriate retention schedule and records classification program for each.

CONCLUSION

The need for compliant RIM best practices is demonstrated daily in all organizations, public and private. Escalating fines and sanctions for poor corporate recordkeeping are evidence that compliant RIM is no longer optional. A program must contain a proactive approach for management of all of the seven Best Practice areas – Accountability, Retention, Policy and Procedures, Imaging, Access and Indexing, Disposal and Compliance. These areas need to be managed consistently and effectively. Organizations are now judged on the implementation of their RIM programs and must strive to demonstrate "good faith" efforts across all aspects of records management. A compliant RIM program must demonstrate the key elements of consistency, accountability, adoption and accessibility. These elements must be audited and updated consistently over the lifespan of the business. By striving to achieve excellence one step at a time in each of the seven Best Practice areas of records management, a comprehensive and compliant program can be implemented across the globe.

IRON MOUNTAIN: PROTECTING AND MANAGING THE WORLD'S INFORMATION

Since 1951, Iron Mountain has been the partner that thousands of companies depend on to store, manage and protect records, media and electronic data in any format, for any length of time. Today, we continue to lead the industry as the only partner you can trust to design and implement a comprehensive and compliant records management program. We have more expertise, resources, experience, proven processes and responsive services to meet your information management challenges now and in the years ahead.

ABOUT IRON MOUNTAIN. Iron Mountain Incorporated (NYSE: IRM) provides information management services that help organizations lower the costs, risks and inefficiencies of managing their physical and digital data. Founded in 1951, Iron Mountain manages billions of information assets, including backup and archival data, electronic records, document imaging, business records, secure shredding, and more, for organizations around the world. Visit the company website at www.ironmountain.com for more information.