A PRACTICAL GUIDE TO INFORMATION GOVERNANCE

PROVEN PRACTICES. NEW THINKING.
ALL IN ONE RESOURCE.

WHITE PAPER

INFORMATION IS...YOUR ADVANTAGE

CONTENTS

WHY READ THIS DOCUMENT?

As you know by now, the volume of information continues to explode exponentially and has become more mobile, making the job of protecting it even more difficult as requirements to do so increase. Most organizations are quickly realizing the need to, and value of, managing information more effectively on an enterprise basis. Traditional activities, such as records management, are no longer sufficient to meet the demands of the business or the ever increasing and more complex current legal and regulatory requirements. The evolution of information management governance is now an essential business requirement to mitigate risk, reduce cost, and increase revenue.

With increasing pressure from the many global regulatory agencies, the need for an Information Governance Program is evolving from a "nice to have" to a "must have." In addition to regulatory, customer, and shareholder pressures, legal discovery requirements continue to become more standardized with courts having less tolerance for noncompliance to established standards and commercially reasonable expectations.

Outside of regulatory compliance, market pressure for increased revenue is driving efforts to find creative ways for organizations to leverage the large volumes of information they retain to increase market share, drive revenue, and maintain a competitive advantage. Without effective enterprise Information Governance, business initiatives such as customer relationship management, knowledge worker collaboration, employee and customer mobility, data mining, big data, enterprise search, data and content analytics cannot be maximized or implemented successfully for enterprise success.

Readers of this paper will find helpful guidance on how to manage information related risks and compliance requirements, as well as develop and implement improved information management and governance processes and practices.

INTRODUCTION

Members of Iron Mountain's Financial Services Customer Advisory Board formed a committee along with Iron Mountain subject matter experts in early 2013 to share best practices around the topic of Information Governance. We started out with the question: What is the best way to construct and maintain an Information Governance Program for our respective companies?

Through our discussions we determined that while each organization shapes and defines what Information Governance means to meet their individual requirements and culture, there are certain elements that are universal. This prompted the committee to create a practical guide with the objective of establishing a common language and an outline of the most critical components and organizational best practices.

METHODOLOGY

Over the past year, the committee members met to discuss and develop a working guide to Information Governance. It is the committee's intention to share its work with records and information management professionals in all industries to use as leverage as they continue to build and refine a robust Information Governance Program. The guide includes the following topics:

- **Definition of Information Governance**
- **Information Governance Principles**
- **Information Governance Model**
- **Roles and Responsibilities of Information Governance Council**
- **The Value of Information Governance**
- **Organizational Best Practices**

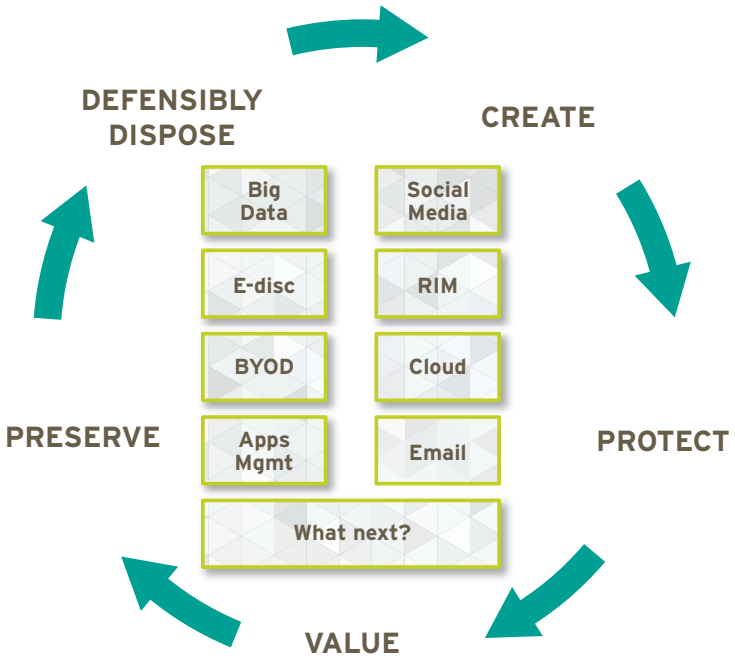
The Information Governance Committee and Iron Mountain are pleased to provide the records and information management community with this guide for developing and maintaining a practical Information Governance Program. This is by no means a definitive, final Information Governance framework. Rather, it is a first step in a journey to develop clarity and guidance on how to approach Information Governance in the context of your particular industry. It is our hope not that you adopt the guide as complete, but use the topics to start an internal dialogue and gain the cross-functional executive buy-in mandatory to support a holistic Information Governance platform.

INFORMATION GOVERNANCE DEFINITION

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.

All too often we see the terms "Information Governance" and "Records and Information Management" used synonymously. While the records and information management function is a part Information Governance, other critical components need to be considered equally.

The associated diagram depicts the various types of content, and its repositories, that are overseen by the activities of Information Governance.



INFORMATION GOVERNANCE PRINCIPLES

It's no secret that initiatives that drive increased operational efficiencies and allow for flexibility to accommodate changing regulations are very popular in today's organizations. Establishing a strong Information Governance Program will allow for just that. A critical first step is to define a set of core principles that will permeate your Information Governance Program and processes. These should include elements such as:

» **Educate** all employees regarding their Information Governance duties and responsibilities.

» **Confirm** the authenticity and integrity of information.

» **Recognize** that the official record is electronic (unless otherwise specified).

» **Store** information in an enterprise-approved system or record-keeping repository.

» **Classify** information under the correct record code.

» **Control** the unnecessary proliferation of information.

» **Dispose** of information when it reaches the end of its legal and operational usefulness.

» **Secure** customer and enterprise confidential/personally identifiable information.

» **Comply** with subpoena, audit, and discovery requests for information.

» **Align** all lines of business systems and applications to Information Governance standards.

» **Ensure** that third parties that hold customer or enterprise information comply with your organization's Enterprise Information Governance standards.

INFORMATION GOVERNANCE MODEL

We know that no two organizations are alike, so rather than put forth a single "best practice" Information Governance Program infrastructure, we set forth in this document the recipe and ingredients that can ensure its successful institution. How your organization combines the ingredients is dependent on your culture, state of maturity, risk profile, current functional orientation, advocacy level, and much more. We encourage you to create your own "ideal" structure that suits your situation today and helps you plan for the future.

There is one common and critical requirement in the formation and sustainability of an Information Governance Program: the sponsorship of an executive, preferably someone within or close to the "C Suite," such as the CIO or General Counsel. Their endorsement of the Program lends a degree of seriousness, expectation, and accountability that will trickle down through the organization. Without such sponsorship, some necessary elements of an Information Governance Program may be overlooked or undervalued.

INFORMATION GOVERNANCE OVERSIGHT

In order for Information Governance to become institutionalized in an organization, it requires guidance and oversight by a cross-functional, senior level Information Governance Council (Council) that meets on a routine basis, at least quarterly. To be most effective, the Council should not exceed 10 individuals. Selected members should be able to represent the functions fulfilled by the following roles, some of which may not exist in your organization. In order to keep the size of the Council to 10 members, certain members may need to be able to represent other roles. For example, your Legal member may be able to speak for the Litigation Officer and the Compliance Officer.

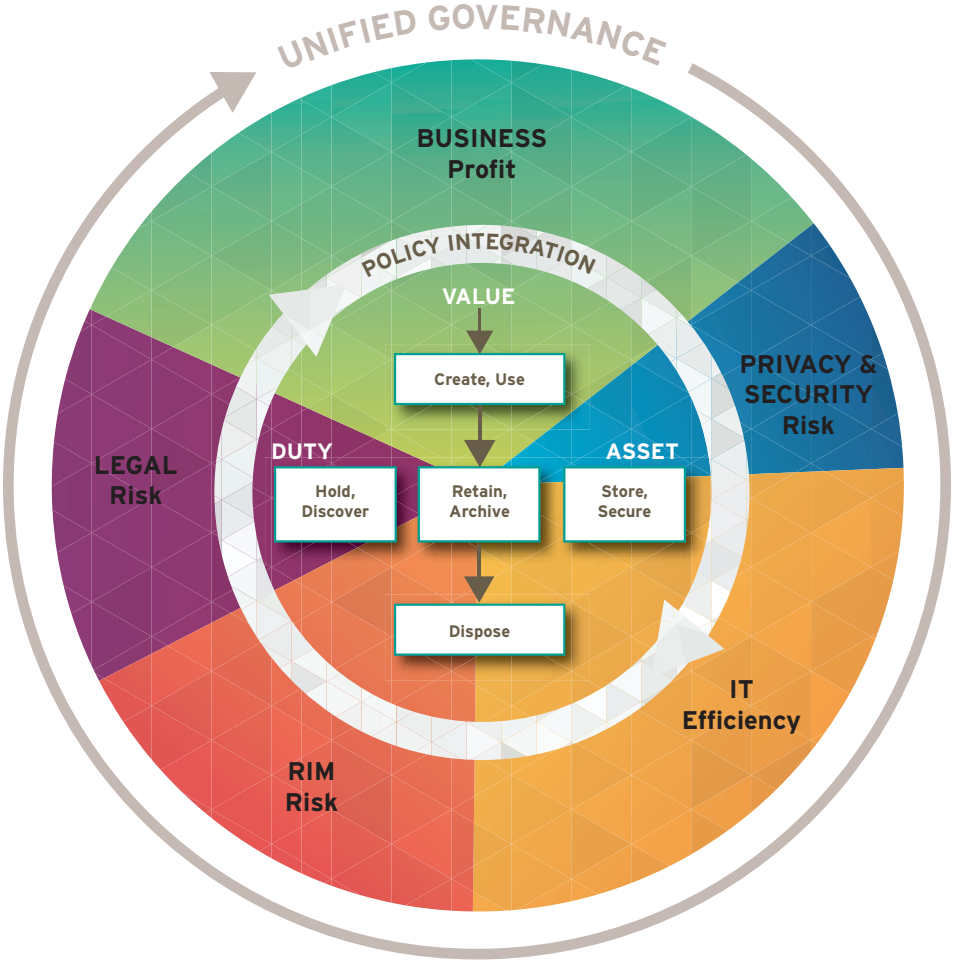
- Executive Sponsor: CIO, or a designee
- Legal (Office of the General Counsel)
- Chief Data Officer
- Chief Health Information Officer
- Discovery or Litigation Officer
- Risk Management
- Compliance Officer
- (Global) Records and Information Manager
- Chief Data Privacy Officer
- Information Technology Security Leader
- Information Technology Infrastructure/Architecture Leader
- Critical Line of Business/Business Unit Leader(s)
- International (Regional) Leaders

The Council is responsible for approving an enterprise-wide Information Governance strategy, developing operating procedures for the Council, providing guidance about technology and standards, assisting in the securing of funds, and advocating the business value of information governance at the C-Suite and Board levels of the organization.

It is important to consider your corporate culture in order to strike the correct balance in the Council membership, participation and collaboration. While support is needed from your most senior leaders, given their span of responsibility, they may not be able to directly manage all of the obligations of the Council. Moreover, it may be best to create sub-committees or other working groups that report into the Council that take responsibility for specific topics or business lines. Through his research, Alan Weintraub, a principal analyst at Forrester, has found that the centralization of the council can be a potential impediment to the line of business' ability to make their own governance decisions. He warns that IT representatives may "try to exert too much control over the information governance process, which can shut out members from the business side from providing input or actively participating in the governance efforts." He also notes that in larger organizations, it may make sense to have more than one Council to fulfill different aspects of Information Governance, such as strategy and daily operational governance.
(TechTarget.com Beth Stackpole, 27 July 2011)

The notion of a multi-tiered Information Governance leadership structure is particularly relevant for industries with varied and numerous lines of business situated within a complex geographical footprint. The executive sponsor or the senior-level Council would determine the need for, and composition of, the subject and/or region specific Councils. In addition, the Councils may assign cross-functional working teams assembled to address a particular topic, such as the creation of standards for line of business self-assessments. In any event, the different tiers of Councils or working teams must be organized in such a way that they roll-up to and are held accountable to the ultimate owner of the Information Governance Program.

INFORMATION GOVERNANCE TYPICAL FUNCTIONS AND ROLES



Source: Information Governance Reference Model / © 2012 / v3.0 / edrm.net

The Information Governance Model (see above diagram) represents the functional areas that are directly responsible for the governance of information across an enterprise. The model weights the involvement of the functional constituents: Business and IT have larger, more complex roles, Legal and RIM slightly less, and Information Privacy and Security share the smallest component as they are more specifically focused in their duties. This is not to minimize the importance that Information Privacy and Security has in the Information Governance model, in fact, in some industries, such as financial services, the Privacy and Security areas will play a greater role due to the abundance of regulations in place to protect the sensitive and confidential nature of information created and received in the course of business.

The following are high-level descriptions of the typical Information Governance responsibilities assigned to the primary functions in the Information Governance Reference Model. In some instances, functions may be

combined within an organization. For example, Legal is frequently where the Compliance and Discovery functions reside, rather than being separate groups within the organization.

LEGAL

The Legal function is responsible for determining the risk profile of an organization based on litigation exposures, international privacy requirements, intellectual property protection, working environment, and more. They should be intimately involved in the development and approval of the organization's records retention schedule and RIM policy; designation of privacy classifications (confidential and public); rules for management of email, social media, mobile devices, and other electronic or networking devices; communication of any changes to the organization through mergers, acquisitions, and divestitures; approvals for defensible disposition; communication to the RIM and IT teams related to any changes to new rules and regulations; and collaboration with key Information Governance stakeholders.

DISCOVERY

The Discovery function is responsible for the communication, instruction, and coordination with business units and/or individuals related to information that must be located, preserved, and produced to satisfy litigation requirements. They may also be responsible for managing Freedom of Information Act requests in countries such as the UK. This function should regularly update designated custodians (typically business owners and IT) on the status of the "holds" on information, including when information can be released for normal lifecycle management; apprise RIM and IT teams when there are any changes to discovery requirements; and institute a repeatable process with associated guidelines to manage the spectrum of simple through complex litigation.

RISK

The Risk function is responsible for the protection of the organization's brand, finances, and operations by managing and mitigating risk exposures. This requires a full understanding of the organization's risk profile (litigation, investigations, regulatory requirements, protection of private information, and protection of intellectual property). They should be involved with Legal in the creation of "acceptable use" policy and with IT to develop acceptable disaster recovery and business continuity processes; selection of SaaS/Cloud providers; provide on-going education of employees regarding prevention of risk-related activities; provide input to Key Risk Indicators; conduct periodic risk assessments; and work closely with RIM, Legal, and IT to destroy information that is no longer required.

COMPLIANCE

The Compliance function is responsible for ensuring that the organization is aware of, and meets the requirements of rules and regulations imposed by a variety of authorities (federal, state/provincial, and local governments; regulatory agencies; data privacy authorities, and industry groups). They should be involved in determining internal metrics and controls; establishing an enterprise-wide audit program; and responding to and managing requests from regulators, auditors, investigators, customers, and other third parties.

RECORDS AND INFORMATION MANAGEMENT

The Records and Information Management (RIM) function is responsible for the development and publication of the RIM Program policy for paper and electronic records. It includes providing implementation support through training and on-going communications; determining and gathering of metrics to determine compliance; cost containment through information lifecycle awareness and storage options, and destruction execution; participation on IT projects for software review and implementation; establishment of a support system for lines of business to include a records coordinator network; staying abreast of trends in RIM (Cloud, big data, and BYOD); and communication/collaboration with key stakeholders to determine policy/approach.

As business-level self-governance becomes institutionalized, the RIM department must create a "self-service" environment from which businesses can "pull" the information they need to comply with RIM Information Governance requirements.

Information Governance will necessitate the evolution of this function from providing records-centric guidance to being inclusive of all information – record or not, physical or electronic.

DATA OFFICE OR DATA GOVERNANCE

The goal of the Chief Data Office function, and specifically the role of the Chief Data Officer (Chief Health Information Officer in the Healthcare Industry), is to assist businesses and other functions in ensuring a consistent and controlled approach to the development and use of enterprise information assets and critical data elements across an organization.

The Chief Data Office is responsible for guiding the establishment of processes and systems sufficient to create, maintain, and share data in compliance with an organization's data standards and external regulations/laws. He or she is the governing authority, along with Enterprise Data Governance Council Members, that implements a framework of controls that support effective and efficient management of data.

The Chief Data Office partners with Data Governance Officers assigned to the functions and businesses across the organization. They conduct data governance/data management practice assessments through various tools such as the Data Maturity Model, Data Quality platform, and Data Standards implementation plans.

INFORMATION TECHNOLOGY

The Information Technology (IT) function is fundamental to the success of Information Governance. While traditionally this function was focused on technology and infrastructure, it is shifting to be more aligned with the business and its objectives. To that end, the Information Governance goal of IT is to increase the ability to efficiently manage the high volume of data being created and received, and to eliminate costs, particularly around redundant technologies and storage. They need to provide leadership for the proper protection and authentication of data and its availability for use, preservation, and disposition. The role also requires collaboration with RIM, Risk, and Compliance to determine appropriate disaster recovery and business continuity plans.

The IT function must collaborate with all other Information Governance roles to understand the requirements of each when it comes to technology selection and deployment.

INFORMATION PRIVACY

The Information Privacy function is responsible for managing the risks and business impacts of privacy laws and policies and responding to regulator and consumer concerns over the use of personally identifiable information, including medical data and financial information, and laws and regulations for the use and safeguarding of information. This role involves selecting and implementing technology as well as staying informed of international privacy law and its impact on records management.

INFORMATION SECURITY

The Information Security function is responsible for the development, implementation, and management of the organization's security vision, strategy, policy, and programs. They are responsible for policy creation; technology selection and implementation; monitoring and informing parties about malware, breaches, hacking, etc.; formally communicating policies and procedures to the business; enabling security standards dictated by customers, such as the government; informing the necessary parties when there are issues with breaches; issuing data classification codes (in conjunction with Legal); and remaining compliant with ISO and other regulatory bodies, as required.

INFORMATION ARCHITECTURE

The Information Architecture function focuses on the organization of information and database development to support the business needs. It includes designing complex, shared information systems; involvement in the selection and management of cloud-based services; support in creating archives for email and social media content; and support for building efficient websites and intranet sites to support RIM.

BUSINESS (OPERATIONS)

The Business (lines of business, business units and/or departments) function is responsible for compliance with the Information Governance policies. The management of information through its lifecycle is most efficient when it acquires the attributes, tags, indices or metadata necessary for compliance as close to its creation as possible. Examples of such metadata are: flagging a piece of information as being confidential, or containing personally identifiable information, or that it is an official business record belonging to a specific category of information. A common complaint of business lines is that records management "gets in the way" of doing business. To that end, IT and RM should work closely with the businesses to determine how they can best take control of their information through technology and process in the least intrusive way.

The line of business is in the best position to determine the "value" of the information they create, maintain, or receive beyond that of its "official" use. Certain types of records may be used to determine marketing trends, track

quality control issues over time, expand customer profiles and identify "bad actors" in a regulated environment. Once again, RIM should work with the businesses to help determine valuable information and how it should be managed in a in a secure and compliant manner.

There is an emerging movement to make business units responsible for self-governance for a variety of corporate requirements or imperatives, including RIM. This is particularly the case in large, geographically dispersed organizations with diverse business lines. The business expectation is to "pull" the information required to self-govern from sources such as RIM and Legal.

INTERNATIONAL REPRESENTATION

Since Information Governance should extend across an organization's entire enterprise, there must be proper geographic representation on the Council. This is most often a representative from a region (i.e., Asia Pacific, EMEA, and North America) that can speak to the concerns of the different jurisdictions within the region.

THE VALUE OF ENTERPRISE INFORMATION GOVERNANCE

The value of an organized and uniformly applied Information Governance Program can be defined in a variety of ways for a variety of audiences – for some, value centers around cost and risk reduction – whereas for others, value is seen as better use of the information itself (e.g. big data). The value question varies not only from organization to organization, but it may vary also from executive to executive, business area to business area, or user to user. Whoever the audience is, gaining buy-in from your organization to establish and fully support the success of your Program can be a challenge.

Value, whether it is true information efficiency or more reliable analytics, is the third rung of the proverbial ladder needed to stand up an Information Governance Program. Risk and cost reduction have traditionally been at the forefront of the value proposition. However, as we have learned over time, the real value of a well-organized Information Governance Program cannot easily be measured using a standard ROI model. Some early attempts at creating Information Governance Programs are met with mixed results due to the fact that the cost savings were overstated. While the Program may have demonstrated "value" in other ways, it failed to produce the promised cost savings thus damaging its reputation. In some instances the true benefit your organization will gain is in protecting and better leveraging the information assets it owns. One of the functions of the cross-functional Council is to establish acceptable goals for information cost, risk mitigation, and organizational value.

THE VALUE OF A DIVERSE COUNCIL

As noted above in the Information Governance Model Functions and Roles section, a true Information Governance Program is more than a Records and Information Management program and should include any and all areas of your institution where information is created and managed. All too often, Information Governance is viewed as starting and stopping with the Records Management and Legal and Compliance functions. By limiting the governance model to only these functional areas, the overall value of an Information Governance Program is diminished. The value of an effective Information Governance Program ultimately stems from the fact that it includes all types of content, from all areas of the organization. An important step is to recognize that each area contributes and interacts with information in different ways and therefore gauges value differently. Below is one example of how different business areas may view the same type of information.

Information should not be kept in functional silos unless policy dictates otherwise. Gaining control over your information is not only valuable to those who manage the lifecycle of the information, but may support the initiatives of other business units across the organization. A strong Information Governance Program can help break down information silos. Cross-functional teams can leverage information that is consistently available, accessible, and most importantly, accurate to create incremental value.

Information can be used in a number of ways. In our conversations with senior information managers at top financial services institutions, we heard several stories, good and bad, about how to position an Information Governance Program for success. The Programs with the greatest amount of success are positioned from a value perspective, demonstrating how information may represent a potential risk but more importantly how it can be used as a strategic asset to deliver value. By examining the information and all its potential uses, you will be better positioned to make consistent Information Governance decisions throughout your institution.

ORGANIZATIONAL BEST PRACTICE

Moving projects and ideas from the Information Governance Council into production is not always an easy task. This section introduces current and emerging processes that have been culled from both real-life successes and failures. The concept of Information Governance is not new, but it is far from being a perfected process. While certainly not an exhaustive list, the following recommendations and insights are put forth to enable or facilitate the various components of Information Governance.

SECURE EXECUTIVE SPONSORSHIP

As recommended earlier, the Information Governance Council is a mix of diverse functions all bringing different functional requirements to the process. One of the most important best practices we can recommend is the designation of an executive sponsor. The lack of a clearly defined executive sponsor is one of the top reasons why earlier attempts at forming an effective Information Governance Program are often unsuccessful.

For some organizations, the recently emerging role of Chief Data Officer is responsible for information lifecycle management as well as sponsorship of the Information Governance Council. This senior executive position provides the level of advocacy needed to ensure that the company stays focused and committed not only to data analytics or data warehousing, but also to the processes that manage and house various types of information (RIM, cloud, email, apps management, big data and social media).

The selection of the Council members must be given special consideration. Its composition should be made up of members of various departments and functional areas, but not the senior most executives. earlier attempts to implement Information Governance Programs have been stalled – or failed – as a result of having senior management with no business line input sitting on the Council. It may make sense to rotate Council members on a periodic basis, for example every 18 - 24 months, to maintain interest.

> "When we started down the path of information lifecycle governance, we thought we needed a steering committee and our consultants confirmed that this was a best practice. But we didn't spend enough time on the front end defining the purpose, scope, and authority of this committee. In the end, we had the wrong people on the committee and we wasted a lot of valuable time. Worst of all, we lost credibility."
>
> Records Manager, Fortune 500
> Insurance and Financial Services

Create real value for one or more businesses and then have them be your spokesperson.

MAKE THE MEETINGS ACTIONABLE

The Information Governance Council should meet regularly, at least quarterly. It is important to get the most out of each meeting by having a clear agenda and ensuring that the concerns of each functional area are addressed. Topics should include a report on key performance indicator metrics (such as number of boxes or bytes of information destroyed, updates on discovery, and its implications on information), consideration of new technology, change management, budget issues, and more. It may be necessary to assign working teams to communicate and put decisions into action, and those teams would report their progress to the Council on a regular basis. Ideally, the Council would develop, publish, and act on a 3 – 5 year strategy for achieving Information Governance objectives.

START SMALL AND SET CLEAR OBJECTIVES

The desire to move on large-scale initiatives and make a splash is tempting. However, we have found that the most successful approach to Information Governance works by starting small, establishing a foundation for a chosen process, then demonstrating and gaining a victory. The selection of the place to start should include considerations of risk, willingness by the process owner to change, and ease of implementation. One example we encountered was that of an institution that began by reviewing the workflow of a single department by taking an inventory of information created and received, building a process that streamlined the management of the information through its lifecycle, and setting goals and metrics for success. In the end, only a handful of records were identified as eligible for destruction but the true "win" was that a process and methodology had been tested and generated quantifiable results. The Council was then able to expand the review methodology to other lines of business, duplicating the process and creating better, more consistent controls across the enterprise.

By starting small and meeting your objectives, you can demonstrate value. It is critical to quantify the value of each program initiative. Whether the initiative is a general clean up or a data mining analysis, the metrics for success need to be in place at the line of business level. Information Governance is a top down and bottom up program that requires senior sponsorship and business area muscle to succeed.

PROVIDE A MECHANISM FOR SELF-ASSESSMENT

While the Information Governance Council should oversee the information lifecycle management policy for the institution, the policy will only be successful if it is adopted and embraced by the broader organization. The value section above helps you evaluate how to modify the way you approach and define value based on your audience, and you may also need to assist individual line of business managers assess their level of compliance with the Information Governance policies endorsed by your Council.

A strong Information Governance framework should therefore include the establishment of a self-assessment program that allows business managers to diagnose their own performance against given controls. A self-assessment program establishes a comprehensive and consistent program for business managers, regardless of their location, to identify and address potential weaknesses in the design or execution of internal processes that mitigate key operational risks and costs. Through the assessment process, lines of businesses will identify problem areas and drive the implementation of corrective actions to resolve or mitigate the potential impact on business objectives and operational risk losses. This process is supported by key functional areas such as RIM, both before the assessment by providing policy and implementation support, and after by assisting in the creation and execution of a remediation plan.

A set of standard controls for the business must be established for the organization by an internal governance authority. While all controls may not be applicable to all lines of business, a set of RIM controls should be mandatory regardless of the function being performed (Human Resources or Retail Banking) or its location (North America or Asia).

All risks associated with the information lifecycle should be managed within the context of policies, procedures, industry standards, and best practices to ensure regulatory compliance and legal requirements are met.

INTERACT WITH LINES OF BUSINESS

It is becoming increasingly clear that the consistent and compliant management of information begins with employees in an organization's lines of business. As such, it is essential that they are given the support they require by the Information Governance functions to be successful. This includes onsite access to clearly written policy (RIM, Information Security, Discovery); periodic training; on-going communication; remediation assistance, when required; guidance for defensible destruction of information; guidance for holding information for litigation; change management tools; and more.

In addition to managing information to remain compliant with regulatory or operational requirements and to contain costs, the lines of business should be engaged in determining the potential use – or value – of the information they create and receive beyond its original purpose. To this end, representatives of the RIM team (and others, such as Marketing or Data Analytics, if required) should reach out to business lines to facilitate the assessment process. A complete understanding of the information managed by the functional area is required – this may already exist in the form of an information or data map or file plan. Considerations for keeping information once it is no longer required to meet retention rules are: use in determining customer trends and requirements, either in general or by individual; demographics; indicators for product expansion; identification of "bad actors;" and more. It is important to keep in mind that other areas of the organization may have use of information that is currently siloed in a line of business. If the decision is made to retain information longer than required by an organization's records retention schedule, it should be approved of by the legal and privacy teams to reduce litigation risk or violation of privacy law.

USE TECHNOLOGY WHENEVER POSSIBLE

Employees have more to do in their work day than to actively manage information at each stage of its lifecycle, from creation and classification through to its destruction. To attain a consistent and compliant information management practice, some degree of automation should be considered. A Gartner report echoes this position:

"As the information landscape continues to expand in scale and pace of change, manual approaches to monitoring data and its uses against information governance policies cannot keep pace..." (Gartner, Inc. G00247985, Make Your Information Infrastructure Governance-Ready)

Data analytics and auto-classification tools are examples of technology that can support the identification and classification of information to attach lifecycle rules and extract its value. Wherever possible, automation should be used to enable the monitoring of self-assessment controls and detection of non-compliance. This is happening today in various functional areas, i.e., monitoring of broker/dealer communications or blocking email from being sent if it contains personally identifiable information, but more will be required in the future. it is the role of the Information Governance Council to help make this actionable.

"As the information landscape continues to expand in scale and pace of change, manual approaches to monitoring data and its uses against Information Governance policies cannot keep pace..."

Gartner, Inc. G00247985,
Make Your Information Infrastructure Governance-Ready

IN CLOSING

Information Governance is a framework that is supported by people, processes, and technology. It is laudable in its effort to pull together what may have been previously disparate functions across an organization in order to create a consistent, compliant, and collaborative approach to managing information for risk, cost, and its value to the organization. The Information Governance Program construction will be different from company to company, but its intent should remain firm.

Information Governance is not a project with a defined time span, but a program with requisite support from executives. Most institutions will go through many iterations implementing and administering the Information Governance Program, including the establishment of a Governance Council. It is important to go into the process with the understanding that there is no "silver bullet" or all-inclusive piece of technology that will provide your institution with instant governance over the entirety of your information.

The Information Governance Program needs to be adaptable as the business and regulatory environments change. Merger, acquisition, and divestiture activity is common in many industries and may result in potential new lines of business, new geographic locations, new technology, cultural and organizational shifts, new members to sit on the Council, and much more. It is important to remember that Information Governance is a framework – it is not static and must reflect current and emerging requirements for the management and use of information as an asset, and potential liability, of the organization.

IRON MOUNTAIN®

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.