A PRACTICAL GUIDE FOR A RECORDS AND INFORMATION MANAGEMENT RISK & CONTROL FRAMEWORK

PROVEN PRACTICES. NEW THINKING.
ALL IN ONE RESOURCE.

WHITE PAPER

INFORMATION IS...YOUR ADVANTAGE

CONTENTS

WHY READ THIS DOCUMENT?

In today's information-driven economy, it's not enough for organizations to say "we know what our information risks are." The newspapers are filled with stories about how improper management and control of information have led to regulatory fines, sanctions, reputation damage and loss of customer trust.

All organizations, and in particular those that are highly regulated, must be proactive in designing a risk mitigation and control methodology that covers all stages of the information lifecycle – from information creation to secure disposal.

The volume of information continues to grow exponentially, making the job of controlling and managing it more and more difficult. We are quickly realizing the need to construct a control framework specifically to address the risks posed by information management. This framework is a vital component of an Information Governance program.

Ensuring that information risks are well understood, documented and then controlled in order to mitigate them are practices that every institution should follow. In addition to external threats, our regulators expect no less.

Readers of this paper will find helpful guidance on controls that must be put in place to manage information-related risks effectively, as well as a suggested risk-rating system for capturing the current status of your organization's control environment.

INTRODUCTION

Members of Iron Mountain's Customer Advisory Board (CAB) formed a Committee in early 2014 to identify and share proven practices around the topic of records and information management (RIM) risk. We started out with the question: "what is the best way to construct, garner support and monitor compliance to RIM policy."

Through our discussions we determined that while each organization shapes and defines how compliance measurement is conducted to meet their individual requirements and culture, there are certain universal RIM risk and control elements. Recognition of this fact prompted the Committee to create this practical *RIM Risk & Control Framework Guide* with the objective of establishing a set of common risk controls to share with their peers as organizations continue to build and refine a robust Information Governance program.

METHODOLOGY

At the onset of our collaboration, the following topics were selected by the Sub-Committee as being essential to the advocacy and development of the framework:

- **Definition of an RIM Risk Framework**
- **Key Drivers for Compliance**
- **Identification of Critical RIM Controls**
- **Institutionalization**
- **Roles and Responsibilities**
- **Measures of Success**
- **Action Plan for Improvement**

The RIM Risk & Control Framework Sub-Committee and Iron Mountain are pleased to provide this Guide for developing and maintaining an RIM Risk & Control Framework for use in institutional compliance and information governance programs. This framework is by no means definitive or final. Rather, it is a first step on a journey to develop clarity and guidance on how to approach proper information compliance. It is our hope that you adopt the Guide to start an internal dialogue to gain the cross-functional executive buy-in mandatory to support your organizational compliance requirements and platform.

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 roles, policies, processes and metrics required to manage the information lifecycle, including defensible disposition.

RECORDS & INFORMATION MANAGEMENT RISK & CONTROL FRAMEWORK

The RIM Risk & Control Framework establishes an operational self-assessment program that allows business managers to diagnose their own performance against a set of given controls. Such a program provides a comprehensive and consistent protocol for business managers, regardless of their location or the work they perform, to identify and address potential weaknesses in the design or execution of internal RIM processes.

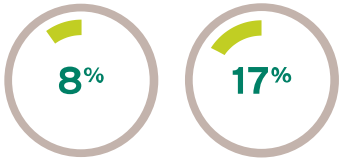
Through a self-assessment process, lines of business can identify problem areas and drive the implementation of corrective actions to prevent, resolve or mitigate key operational, legal, compliance and reputational risks and costs. This process is supported by key functional areas such as RIM, Compliance, IT, Information Security and Privacy and Internal Audit to provide input to the creation of the program. It also helps to support its implementation and to assist in the creation and execution of a remediation plan after assessments have taken place.

All risks associated with the information life cycle must be managed within the context of policies, procedures, industry standards and best or proven practices to ensure that regulatory, operational, compliance and legal requirements are met.

The RIM Risk & Control Framework should be positioned as a component of a broader set of organization-wide compliance controls. Organizational compliance is described as an enterprise's "tangible efforts to prevent, detect and otherwise respond appropriately to wrongful behavior associated with the actions of those working on an organization's behalf. This includes directors, officers, employees, agents and independent contractors."[1]

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

DRIVERS



Only 8% of organizations use metrics to "inspect what they expect" and only 17% conduct RIM compliance audits.

The compelling reasons for instituting an RIM Risk & Control Framework are in some cases universal and in others specific to a region or individual jurisdiction.

Universally, the ability to provide proof of proper risk management and compliance protocols for regulatory bodies, customers and auditors is a major driver. Yet, according to the 2013|2014 Cohasset/ARMA Information Governance Benchmark report, only 8% of organizations indicate the use of some form of metrics to track RIM activity and a mere 17% conduct RIM compliance audits. In addition to these low numbers, only 7% of the survey respondents claim that their employees are engaged in their RIM programs.

Only 7% report employees are engaged in RIM.

Examples of drivers include general and industry-specific compliance laws and data privacy obligations. In the United States, regulations include the Dodd-Frank Act, Payment Card Industry Data Security Standard (PCI DSS) , Health Insurance Portability and Accountability Act (HIPAA), the Federal Information Security Management Act (FISMA) and the Sarbanes-Oxley Act (SOX). In the EU, the Financial Conduct Authority (FCA) and Prudential Regulatory Authority (PRA) are prime examples. The European Union General Data Protection Regulation (GDPR) that is set to replace the 1995 Data Protection Directive (EU Directive 95-46-EU) is another strong motivation for implementing an RIM Risk & Control Framework.

Given the multitude of drivers and our current inability to track or measure policy compliance to mitigate that risk, there is a substantial gap to be filled between an organization's commitment to managing information and proof of actual practice.

It is unrealistic to expect resource constrained RIM staff to police the entire organization, especially when the volume and variety of electronic records is factored into the information management equation. Therefore, a new method of engaging the lines of business responsible for the creation, receipt, maintenance and disposition of information must be devised and implemented. Evidence of their compliance to a base line set of mandatory Controls will strengthen an institution's compliance profile and lead to mitigation and/or remediation plans, as required into the information management equation. Therefore, a new method of engaging the lines of business responsible for the creation, receipt, maintenance and disposition of information must be devised and implemented. Evidence of their compliance to a base line set of mandatory controls will strengthen an institution's compliance profile and lead to mitigation and/or remediation plans, as required.

RIM RISK CONTROLS

There are nine major categories of RIM Risk Controls featured in this Guide that address the management of information through its lifecycle. They are:

» **Governance**

» **Inventory**

» **Retention**

» **Disposition**

» **Legal Holds**

» **Privacy and Security**

» **Vendor Management**

» **Staffing**

» **Training**

For each category we give a brief description that is followed by a table. The table is comprised of four elements:

Control: A standard of performance within the category that has been designated as critical to the RIM Risk Assessment process.

Description: An explanation of the meaning and relevance of the control.

Supporting Information: Additional guidance as to specific actions for evaluation that is associated with the control.

Rating: Guidance for assigning an assessment value to the control to be used in determining the level of line of business compliance. It is expected that the line of business respondent will select a number from one – four based on its actual adherence to the control (one is the highest attainable rank, four the lowest). Bear in mind that not all lines of business may need to achieve the highest rating for all of the controls.

GOVERNANCE

Governance is the overarching management and accountability structure for a compliant RIM function. While these controls can be relevant for all lines of business or at a corporate level, they are provided below as they would specifically relate to the governance of the RIM function.

CONTROL	DESCRIPTION	SUPPORTING INFORMATION	RATING
Management Review and Oversight	Management of the RIM function is actively engaged and accountable for daily conduct of RIM operations. Risk management oversight committees exist to monitor RIM program status (e. g. , Information Governance Council, Information Risk Committees). Significant operational issues, business process, risk capacity, infrastructure, legal, compliance and regulatory control concerns are reviewed, documented and addressed in a timely manner.	– Information Governance Council or its equivalent is convened on a regular basis. – Attendees include representation from all relevant disciplines, e. g. , senior management of RIM, Risk, Legal, Compliance, Information Security, Audit, etc. – Timely production of agenda and minutes are generated as evidence of meeting attendance and decisions made. – Follow up actions are documented and addressed at subsequent sessions. – Significant accountability and control concerns are reviewed and escalated as appropriate.	1. RIM oversight committee(s) exists with senior membership sponsorship and attendance. Clear set of goals identified and communicated. Decisions and assigned accountability are documented and monitored. 2. Oversight committee(s) exists with senior membership attendance but they cannot demonstrate accountability and decisions through documented actions. 3. Limited committees exist with limited membership. Meetings are inconsistent and while repeatable actions occur, there is limited evidence found in supporting documentation. 4. No RIM-related committee exists.
Policy and Procedure Management	RIM policies are created and managed in accordance with the organization's policy management process. Standard Operating Procedures for RIM clearly outline the functions to be performed and controls to be executed and evidenced when parties interact with the RIM process.	– Management of RIM Policy and Procedures must be supported by a designated senior level person/ team accountable for the contents of the policy and supporting procedures. – Scheduled review and update is conducted within a documented process to approve, amend, supersede and decommission policies. – An inventory of all policies owned and managed by RIM exists and published versions of policies are archived in accordance with the Records Retention Schedule. – Evidence of proper policy management includes version control, meeting minutes, documentation of approval of revisions and decommissioned or superseded policies. – Procedures are reviewed at appropriate frequency to ensure instructions remain accurate and up to date.	1. RIM policies and procedures are kept up-to-date, approved by relevant authorities and made available to key decision makers and affected parties. Superseded and decommissioned versions are archived and retained per the applicable Records Retention Schedule. 2. RIM policies and procedures are updated regularly and shared with relevant parties, but superseded and decommissioned versions are not appropriately updated. 3. RIM policies and procedures exist but are not updated regularly or are not approved by the appropriate authority or are incomplete. There is no formal and consistent way to share updates. 4. No formal RIM policies or procedures exist.

Legal / Regulatory Change Management Process	New/updated regulations and legislation are monitored for applicability to RIM Program, especially those that impact Records Retention Schedule(s). Legal, Compliance, RIM, LOB management (and others , such as third parties, depending on the nature of the issue) are engaged to assess impact to the business. Policies, procedures and Records Retention Schedules are evaluated and revised in a timely manner. Staff training is refreshed as required.	– The Legal, Compliance and/or RIM teams have an established process in place to receive information regarding pending or promulgated legislative or regulatory changes that would affect the RIM Program.	1. A formal process exists for identification and review of changing legal and regulatory requirements that affect the RIM Program. 2. Legal and Compliance teams review changes periodically but do not consistently inform the RIM unit of all changes affecting RIM operations. 3. Legal and Regulatory changes affecting the RIM Program are identified on an ad hoc basis and dissemination of requirements is inconsistent. 4. There is no formal process for identification, amendment or communication of changes to regulations and legislation affecting the RIM Program.
RIM Tools Governance	Tools used by the RIM team (such as inventory tracking tools) or by LOBs in order to manage RIM policies (such as Electronic Records Management tools) are approved according to all IT governance protocols. All RIM tools are properly identified and captured in the organization's application inventory tool (see Inventory Controls). These RIM tools must be risk-classified and subject to ongoing assessments to validate their design and confirm they achieve their stated functionality and purpose.	– All tools used in the RIM process must conform to organizational policies and standards so as to minimize risk of data loss, unauthorized access or uncontrolled changes. – RIM tools require proper oversight and controls to appropriately support RIM and business unit activities and reduce risk to the firm.	1. The RIM Program periodically reviews its tools against corporate IT criteria and ensures they are included in the organization's application map. The tools are risk classified. 2. Some of the RIM Program tools do not have a risk rating or only partially conform to IT standards. 3. The RIM program has some ratings but does not conform to policy or IT standards 4. The RIM tools do not conform to IT standards or there are no periodic reviews or risk ratings. The tools are not included in the application map.

INVENTORY

The organization's ability to know what records exist across the enterprise, in any format and where they are stored is reflected in an inventory.

CONTROL	DESCRIPTION	SUPPORTING INFORMATION	RATING
Physical Records: Inventory Tracking	Physical records in all locations, onsite and offsite, in which the company operates, must be inventoried. A centralized inventory listing ensures the proper oversight and control of physical records.	– Physical records inventory tracking captures and reports the following data points for boxes and/or files: vendor or internal storage area name, location, department, box/file count, destruction eligibility, valid/invalid record codes or series, boxes/files subject to Legal or other Holds, boxes/files past due for destruction, boxes/files missing identifying data, recalled boxes/files not returned after 90 days.	1. Physical records inventory is comprehensive (all vendors and all company locations included) and contains all of the suggested data points. It is housed in a centralized database, which can be easily queried. 2. Physical inventory contains most of the suggested data points, but may not be on a centralized database. Some compilation exercises must be done to produce a unified view of the entire inventory. 3. There is no centralized inventory for physical records. Inventory tracking for multiple vendors exists but is largely driven by vendor owned systems and parameters. 4. There is no tracking of physical records inventory.
Digital Records: Inventory / Data Map	A complete and accurate inventory of all company applications and a comprehensive data map is critical to the ability to manage electronic records. Such an inventory must cover structured, semi-structured and unstructured data repositories where records could reside. It must be kept up-to-date to be effective.	– The data map encompasses all Electronically Stored Information (ESI) as defined in the Sedona Principles. https://thesedonaconference.org/publication/The%20Sedona%20Principles. – The companion application map includes all applications, systems and repositories of records across the enterprise. – Scheduled maintenance is conducted to ensure accuracy of the inventory and map.	1. A complete and accurate inventory of all company applications exists and a data map includes all ESI that exists. It is updated on a routine, scheduled basis. 2. There is an inventory of all applications but it is not accurate and/or updated periodically. 3. In order to get a complete picture of all applications, several sources must be referenced. Data map is incomplete/does not include all ESI. 4. No application or data map exists.

Line of Business (LOB) Records Indexing	Taking guidance from the RIM team, each LOB must develop a records index in sufficient detail to fully support Legal Hold, e-Discovery and records retrieval processes for paper and electronic content. This indexing includes the appropriate records classification and storage location for each identified record.	– LOB indexing reflects the use of the appropriate record code/record class from the company retention schedule(s). – Indexing provides sufficient supporting information so as to be able to consistently retrieve records in a timely fashion when needed, place Legal Holds on material responsive to Hold Notices or for e-Discovery purposes.	1. LOBs maintain complete and accurate indexing of all records, both physical and electronic and can respond to Legal Hold notices or requests to produce information, in a timely and efficient manner. LOBs perform self-audits at least annually to reconcile vendor indexing with LOB indexing of physical records. Changes made to Records Retention Schedules are updated accordingly. 2. LOBs maintain an index of records but it is not fully complete, accurate or updated periodically to reflect changes to the company retention schedules. 3. LOBs maintain some indexing, but it does not capture all of the electronic and physical records. It may be largely focused on physical records and does not reflect the requirements of the current Records Retention Schedules. 4. LOB does not maintain any index other than what is in physical records vendor tracking inventories and/or data maps.

RETENTION

Retention is the foundational requirement of managing records, in any format, according to laws, regulations and operational obligations. This activity includes the classification of records to enable assignment of retention rules.

CONTROL	DESCRIPTION	SUPPORTING INFORMATION	RATING
Records Retention Schedule	A Records Retention Schedule supports compliant management and classification of records across all formats, LOBs and jurisdictions. The schedule uses legal and regulatory citations, laws and rules, as well as operational requirements to indicate the length of time for which records must be retained. It is published and widely accessible for employee use.	– A centralized, enterprise-wide, legally defensible Records Retention Schedule is created and maintained. Its basis is the legal research, subjective opinion from legal or other authorized staff and operational overrides. – The retention period for each record class is documented and maintained in such a way that it can be produced and reviewed. – Legal research for each applicable jurisdiction is updated and reviewed on regular scheduled basis. – A process exists to handle legal or regulatory changes that could impact the Retention Schedule. – Changes to the Schedule must be communicated to all stakeholders. – A reportable audit trail exists for all changes made to Retention Schedules.	1. Enterprise Records Retention Schedules for all jurisdictions have been developed and are reviewed, updated at a regularly scheduled time (at least once a year) and published to stakeholders. 2. Enterprise Records Retention Schedules for all jurisdictions have been developed and are reviewed, updated periodically (not scheduled or within a year) or infrequently and published to stakeholders. 3. The firm has multiple LOB-created Schedules (no enterprise-wide version), which are updated regularly. 4. No Schedule exists to document the classification of records or retention rules.
Scheduled Review / Archive Event	There must be a scheduled review of physical and electronic records to determine lifecycle stage and appropriate retention management action: deletion, archive, send to offsite storage, shred, etc. This periodic review uses the records retention schedule to identify business records and length of time for retention. Review is annual, at a minimum.	– Each LOB conducts a scheduled review(s)/archive event(s). – Inactive records are archived and records with no ongoing business or legal value that have met their stated retention are destroyed. – All employees who store or manage records are expected to take part and written instructions for the storage, preservation or disposition of records is provided for paper and electronic content. – Employees attest that they have completed a review of their paper and electronic records and followed the instructions for the storage, preservation or disposition of their records.	1. Scheduled review and archive of paper and electronic records occurs and appropriate action taken. Employee attestation is systematically documented and captured. 2. Scheduled review of paper records with action taken. No review of electronic records. Employee attestation is systematically documented and captured. 3. Periodic review of paper and electronic records occurs with random and inconsistent action taken. 4. While periodic review is in the RIM Policy, no review or archiving takes place for any records.

Review of Back-Up Media	Scheduled reviews of backup media (a copy of data stored for purposes of restoration in the event of a data loss) are undertaken to ensure duplicate records are not retained longer than the official record.	– The RIM Program creates policies and conduct-related monitoring activities to ensure backup media are created and used for disaster recovery purposes only. – Backup media are not used as a records retention repository or archived unless approved by a designated authority (RIM, Legal, Compliance).	1. Policy exists to define use of backup tapes for disaster recovery purposes, not as an archive, unless authorized. Process exists to synchronize management and monitoring of official version of record with copies on backup media. 2. Policy exists to define proper use of backup tapes for disaster recovery purpose. There is no action taken to prevent the duplicate storage of records. 3. No routine exists to reconcile official version of record with backup copies. 4. Backup tapes are not reviewed or destroyed.

DISPOSITION

Disposition relates to a decision made about a record that has met the end of its required retention period per the organization's formal records retention schedule. A record may be destroyed, moved to an archive for long-term preservation or designated as valuable beyond its original purpose for use in data analytics.

CONTROL	DESCRIPTION	SUPPORTING INFORMATION	RATING
Secure Destruction of Eligible Records	Records eligible for destruction are securely disposed of in accordance with RIM Policy and Information Security protocols.	– Roles and responsibilities of the secure disposition process are clearly defined and communicated in policy and procedure. – Electronic data or physical record secure destruction standards are upheld consistently and audited.	1. All eligible records are disposed of routinely and securely. The process is documented and regularly audited. 2. Eligible records are disposed of securely, but the process is not audited or discrepancies have been found in the process. 3. Some, but not all, eligible records are securely destroyed or there is no confirmation in writing of the secure destruction. 4. Records are not disposed of in a secure manner.
Destruction Suspension	The destruction of records under legal or administrative hold is suspended while the hold is in place. Records that become eligible for destruction while under hold cannot be destroyed until the hold is removed.	– Roles and responsibilities of the Legal Hold process are clearly defined and communicated. – Once an eligible record is released from a Legal or administrative Hold, normal disposition processes commence.	1. Legal Hold protocols are followed and disposition process engaged upon release of the Hold. 2. Legal Hold protocols are followed, but normal disposition does not commence on a timely basis upon lifting of the Hold. 3. Legal Hold process is not followed. 4. There is no Legal Hold process.

LEGAL HOLDS

Legal Holds are used to suspend the retention requirements and cease destruction of certain groups of records, even if they are eligible for destruction.

CONTROL	DESCRIPTION	SUPPORTING INFORMATION	RATING
Legal Hold Policy and Process	Legal, in partnership with Compliance, IT and RIM, establish and implement an end-to-end Legal Hold process to include policies and procedures for enforcing preservation obligations for paper and electronic records. Performance measures and roles and responsibilities are clearly documented, including that of a Global Hold Management Response team.	– Document the end-to-end Legal Hold process, either using a flow chart or some other comprehensive means. – The process includes a method for suspending destruction of records required for litigation and removing Holds when the matter has concluded. – Create clearly defined roles and responsibilities for the Hold process: determine participation on a Global Litigation Response Team (Legal, IT, RIM, Business Leadership and Outside Counsel as needed) for each region. – Conduct Hold process training for individuals with a role and responsibilities.	1. An end-to-end Legal Hold process with associated policies and procedures, including roles and responsibilities, exists and is regularly updated, as required. Training occurs for participants. 2. A Legal Hold process and policy exist but there are no formally defined roles and responsibilities. 3. A Legal Hold process exists but no policy supports formal roles and responsibilities. 4. No formal Legal Hold process, policies or procedures exist.
Hold Management	Legal, RIM, Compliance and IT must collectively create or select, utilize and monitor a central authority for the management of Legal or other types of Holds according to the Legal Hold Policy and Process.	– The central authority system includes information about Holds such as: Hold identification code, custodians, application owners, applications, record content and features of systems/processes that may prevent identification and/or retention of potentially discoverable information. – RIM assists in the selection and maintenance of an application for managing Holds.	1. A central authority system/application exists to manage the Hold process. 2. The Hold process is managed manually by a central authority. 3. Holds are managed manually by multiple areas or businesses 4. There is no active management of Holds.
Hold Execution	RIM must be aligned with the Litigation and Regulatory Investigation teams to ensure consistency, comprehensiveness and compliance with the Legal Hold process.	– RIM supports the preservation (and collection and production) of responsive records, removal of Holds when no longer required and the return of records to their normal, "business as usual," disposition per the organization's Retention Schedule based on instructions from a Legal Hold Coordinator or other designated source. – RIM works closely with LOBs and IT to ensure appropriate actions are taken to both places and lift the Holds.	1. The Legal Hold process is complied with to the fullest by all required parties. RIM is actively involved in both the placement and lifting of Holds, at the direction of the Legal Hold Coordinator. 2. There is no Legal Hold Coordinator. Litigation team works directly with RIM to execute holds. 3. Legal Holds are placed and lifted without RIM involvement. 4. There is no Legal Hold process in place..

Hold Scope	The RIM Program helps to ensure that Holds are placed as narrowly as possible. Broad "blanket Holds" are discouraged except if absolutely necessary.	– The entity issuing the Hold Notice should use structured interviews and questionnaires, where possible, to aid in relevant document/data scoping during the course of a matter. – Capture results in the central repository. – Ensure that Legal Hold Notices are written by attorneys in a manner that: • assists persons in taking actions and provides additional instruction (e. g. , aligning the hold notice with record categories in the Records Retention Schedule) • create and use templates for consistent communication of instructions both initially and when scope increases or decreases.	1. Holds are focused only on records deemed relevant to a matter. 2. Efforts are made to prevent blanket Holds and/or remove not relevant records from current blanket Holds. 3. Blanket Holds are the norm. 4. There is no Legal Hold process in place.

PRIVACY AND SECURITY

Privacy and Security Controls relate to the actions required to protect information according to laws, regulations and operational requirements throughout its lifecycle.

CONTROL	DESCRIPTION	SUPPORTING INFORMATION	RATING
Data Classification	Information is classified according to the sensitivity and value that it has to the organization. Information security controls must be put in place commensurate with the classification of the data.	– Examples of data classifications: • Highly Confidential, which includes Personally Identifiable Information (PII) • Confidential, Restricted or Internal Use Only • Unrestricted or Public	1. All information in the company is classified and data protection controls are in place commensurate with the sensitivity and value of the information. 2. Company data is only partially classified and protected. The focus of protection is on PII and other Highly Confidential Information. 3. No formal information classification protocols, but sensitive data is protected on some level. 4. No data classification and protection policy or process exists.
Secure Access	In order to keep information secure, measures must be put in place to safeguard information in all formats. The RIM policy may address these safeguards or they may be addressed in a separate information protection policy.	– Systems must be safeguarded with access controls that include password protection for access to systems. – Passwords should follow a format that is hard to "guess" for added protection. An example of an acceptable format might be: password must be unique, at least 8 characters in length, with at least one letter and one number or special character (!,@,#,$,%,^,&,*,[,]). – Passwords should be changed on a scheduled basis. – Automatic screen savers are enabled on systems that are inactive for a specified period of time. – Physical records are kept in a safe and secure environment, including lockable storage systems and keycard access for storage areas.	1. System access is controlled by password protection in hard to guess formats, automatic screensavers are enabled after 10-15 minutes of inactivity, hard copy records are in locked cabinets/rooms or in location requiring keycard access. 2. System access is controlled by password protection, users are asked to lock computer with Ctrl/Alt/Del function when not in use, hard copy records are in locked cabinets/rooms/locations. 3. System access is controlled by password protection; hard copy records are kept in various locations but may not always be appropriately secured. 4. System access is controlled by password protection; no controls in place for protection of hard copy records.

Cyber Security (Data Protection)	In order to mitigate the risk of data loss, adequate and commensurate prevention techniques must be in place. The RIM policy may address these data protection protocols or they may be addressed in a separate information security/privacy/ protection policy.	– Data encryption on data in transit and at rest must be instituted for sensitive and private information. – Encryption must be enabled on all mobile devices in case of theft. – USB restriction on removable media (thumb drives, laptops, etc.) is strongly recommended.	1. The most up-to-date cyber security tools and processes are in place. Data protection policies exist. 2. Cyber security tools are in place but may not be "state of the art." Policies exist. 3. Data protection policies exist but tools are out of date or non-existent. 4. There are no policies or tools for data protection.
Secure Shredding	A secure shredding protocol is implemented to protect the organization from data loss due to theft or inadvertent disclosure of confidential paper documents.	– The RIM Program creates, publishes and implements a shred-all policy that assumes all paper records are confidential and therefore required to be shredded.	1. Shred-all policy in place for all paper records. 2. Shred-all policy in place for paper records marked as Highly Confidential, Confidential or Restricted. 3. Shred-all policy in place for Highly Confidential and Confidential only. 4. No shred-all policy in place.
Media & E-Waste Disposal (IT Asset Disposition)	To protect from data loss due to theft or inadvertent disclosure of confidential information contained on different types of media, the RIM policy or a separate information protection policy, outlines the requirements for the secure disposal of digital media.	– Establish a defensible, documented and repeatable process to prepare, transport and destroy hard drives, backup tapes and other e-waste either at the firm's data center or at an offsite destruction facility of a third-party vendor. – Audit the process, with certification of chain of custody and strict adherence to industry and municipal mandates for safe disposal of IT assets.	1. A third-party vendor is contracted that specializes in secure media and e-waste disposal for hard drives, backup tapes and other hardware or equipment that contains information. Vendor process must be auditable, with certification of chain of custody and final disposal. 2. A third-party vendor is contracted that specializes in secure media and e-waste disposal. There is no audit trail. 3. No formal process exists to securely destroy media and e-waste.
Data Breach Incident Reporting	Data breach incidents are discovered and reported to the appropriate Incident Response Team in a timely manner and incidents are analyzed to ensure proper investigation, containment and control. If necessary, notification is sent to regulator(s), law enforcement and affected customers.	– Global Privacy Policy and Incident Reporting policy exist to describe the process of managing each step of reporting data breaches.	1. Data Breach Policy and Protocols are rigorously adhered to. An Incident Response Team exists. 2. Data Breach Policy and Protocols are rigorously adhered to but there is no coordinating Incident Response Team. 3. Data Breach Policy and Protocols exist but compliance is inconsistent. There is no Incident Response Team. 4. No data breach policy exists.

VENDOR MANAGEMENT

Appropriate selection and management of third-party vendors is mandatory to ensure that vendors are in compliance with the organization's RIM policies and standards with respect to the management of records and information.

CONTROL	DESCRIPTION	SUPPORTING INFORMATION	RATING
Vendor Selection Due Diligence	The RIM Program undertakes an appropriate level of due diligence for each third-party vendor, in compliance with RIM Policy requirements and the organization's overall procurement/ vendor selection process.	– Adequate internal/external due diligence is undertaken with the involvement of all necessary disciplines (Risk, LOB, Legal, RIM, etc.) prior to conducting business. – Evidence exists that the vendor can comply with RIM Policy requirements for storage, protection, secure destruction, etc., including site visits, references, etc. – Due diligence results are documented.	1. Due diligence occurs involving all relevant parties and is fully documented. Evidence is gathered to prove vendor can meet RIM requirements. 2. Due diligence occurs involving all relevant parties and is fully documented. No evidence of compliance exists. 3. Due diligence occurs but may not include all parties or be fully documented. 4. There is no formal due diligence process for vetting RIM vendors/partners.
Vendor Assessment	The RIM Program must measure service risk, assess controls and supervise performance for technology, operations, partnerships and other vendor and/or third-party relationships such as offsite storage that assist in RIM processes. An executed and valid contract defines the scope, obligations and responsibilities of the parties. Services and scope performed by vendors are proven to be consistent with the terms and conditions of the contract on a scheduled basis.	– Roles and responsibilities are defined for vendor supervision and governance that includes decision making, escalation and oversight. – A Service Risk Manager is assigned for managing day-to-day contract obligations. – Evidence exists, including site visits, to support vendor supervision to include regular meeting minutes that document service level agreement performance, risks, issues, remediation plans, sub-contractors organizational changes and financial health. – Vendor services are managed and monitored according to outsourcing, auditing and supervisory requirements.	1. Scheduled and formal vendor assessments occur during which time services are reviewed and remediation plans documented and tracked. 2. Periodic assessments of all vendors are performed and remediation plans documented and tracked. 3. Assessments are performed for some vendors but there is no consistent follow-up for remediation. 4. No risk assessment of RIM vendors occurs.

STAFFING

Staffing relates to the personnel required to administer, maintain and support the RIM program wherever business is conducted, both as an independent function and within lines of business.

CONTROL	DESCRIPTION	SUPPORTING INFORMATION	RATING
RIM Staffing: Dedicated	The RIM program is staffed with full-time individuals operating globally, as required, with the support and oversight of senior leadership.	– Centralized RIM governance exists and is staffed with the necessary number of dedicated, full-time, trained/certified individuals to ensure program implementation, maintenance and collaboration with other functions such as Legal, LOBs and IT. – If the program is not centralized, authority is given to an appointed individual(s) to develop and manage the program and relationships. – Staffing changes are made as the program expands or contracts are made.	1. Dedicated full-time, centralized, trained and certified RIM staff exists in adequate numbers to run the program and is supported by senior leadership. 2. Dedicated full-time centralized RIM staff exists but in insufficient numbers to be fully effective. Minimal senior leadership support. 3. Insufficient numbers of dedicated full-time centralized RIM staff exist. No senior leadership support. 4. No dedicated full-time RIM staff exists.
RIM Staffing: Network (Part Time)	Staff in LOBs is assigned to support the centralized RIM program locally in addition to their full-time jobs. This role as LOB Records Coordinators or Contacts is outlined in the RIM Policy as a requirement that the LOBs must meet in order to be compliant in their RIM practices.	– Decentralized LOB coordinator roles are created and maintained. – Staff is assigned and maintained to support the centralized program and serve as points of contact for centralized staff. – Changes to LOB coordinator assignments are reported to centralized RIM staff. – RIM responsibilities are factored into coordinator annual goals and objectives.	1. Decentralized LOB staff is allocated to support roles. Open lines of communication with centralized program exist. 2. Some, but not all, LOBs have support staff. Open lines of communication with centralized program exist. 3. Some LOB support staff exists with no connection to centralized program. 4. No RIM support staff exists in LOBs.

TRAINING

The development, delivery and monitoring of training for all employees and others (contractors or vendors) who create, receive and/or manage records and information is essential to support compliance with RIM policy.

CONTROL	DESCRIPTION	SUPPORTING INFORMATION	RATING
Develop Training and Communication Plans and Materials	Appropriate training plans and materials are developed, maintained and approved by an authorized individual or function. On-going communication occurs to re-enforce training and inform of compliance requirements, changes to policy, etc. The RIM Program should serve as subject matter experts on any RIM-related training.	– Periodically review training materials for accuracy and submit requested changes to authorized individual or function. – Work with communications team to ensure employees are kept up-to-date with policy changes. – If no communication team exists, develop a plan to build awareness and implement.	1. Plans and materials are up-to-date and approved on a scheduled basis. Dedicated staff ensures that on-going communication to all employees occurs persistently and consistently. 2. Plans and materials are up-to-date and approved. On-going communication is inconsistent or non-existent. 3. Plans and materials are outdated and administered ad hoc. 4. Plans and materials do not exist for RIM training.
Train and Monitor	Evidence exists of notification to intended training recipients and successful completion of course material. Adherence to required training plans is monitored and attendance is enforced by training sponsors.	– Confirm accuracy of list of training attendees. – Provide evidence of substantiation including master list of training candidates indicating course completion or not, along with communication and follow-up in centralized repository.	1. All employees wherever business is conducted have completed courses successfully with supporting evidence. 2. Selective employees requiring training have completed courses successfully with supporting evidence. 3. Inconsistent training and enforcement of successful completion. 4. No RIM-related training occurs.

It is important to note that most regulated organizations require each line of business to develop an overall Risk and Control Self-Assessment (RCSA) that documents, assesses and quantifies all of the risks the business faces.

INSTITUTIONALIZATION

The RIM Risk & Control Framework is intended to ensure that organizations are in compliance with laws and regulations for the management of records in all lines of business in all geographies. It does so by encouraging the establishment and institution of a set of controls that serve to mitigate a variety of records and information risks.

Your organization's RIM team must review the proposed controls to determine which are appropriate to your specific operation. It is highly recommended that the selected controls be discussed with other teams within your organization, such as Compliance, Legal, Information Security and Risk Management, to ensure the consistency of approach, obtain their "buy-in," and to avoid any potential redundancy with their initiatives.

Once the controls are agreed upon, the RIM team must communicate to the lines of business the purpose of the controls, the process by which they are distributed, instructions for consistent RIM Risk Assessment ratings and other pertinent information. Online access to this information will facilitate the dissemination of valuable information at the onset of the self-assessments and for continuing reference. You may consider conducting a "pilot" with one or two lines of business before launching the control self-assessment across the enterprise.

It is important to note that most organizations require each line of business to develop an overall Risk and Control Self-Assessment (RCSA) that documents, assesses and quantifies all of the risks the business faces. The RIM Controls described in the previous section can form a critical piece of this RCSA document.

FRAMEWORK OVERSIGHT

Line of business RIM Risk self-assessments must be completed on an annual (or otherwise designated) cycle. To ensure that they remain synchronized with compliance requirements or reflect material changes to the business, it is critical to establish a formal process for review and maintenance.

The following describes a multi-phased approach to update and secure approval by relevant and authorized parties, for example, RIM, Compliance and global lines of business, to confirm that the risk and control ratings and their system of delivery, remain appropriate.

Annually:

- Identify any new risks, add or modify controls
- Confirm applicability of current controls, edit as required
- Review input from the lines of business related to ease of use of collection tool, relevance of controls and rating system
- Make appropriate changes to the RIM Risk Assessment process
- Monitor methodology

Quarterly:

- Assess how controls are functioning
- Recommend changes, as required

Continuous:

- Identify gaps in the RIM Risk and Controls Framework assessment design and execution
- Receive input from lines of business
- Recommend changes, as required

It is important to document the decisions taken to edit or augment the RIM Risk Controls and their deployment to the lines of business. Attention must be given to the adherence of the frequency of reviews, the creation of an action plan if target dates are missed and the timely capture of new or emerging risk events. Depending on the needs of an organization, a less rigorous schedule to review the RIM Risk Controls may be sufficient.

METHOD OF DELIVERY

The method for the RIM Risk self-assessment data collection should provide evidence of submission to and compliance by, the lines of business.

The ideal delivery mechanism for pushing RIM Risk self-assessments to designated line of business managers is technology-based. This mechanism can take the form of the SurveyMonkey® online survey tool or similar application that enables an interactive user experience, complete with instructions for responding within a prescribed time frame. It must also provide reporting on results for use by the RIM team and others who are involved in the evaluation of the assessment ratings and remediation process. If technology is not available, other options for dissemination, tracking response times and collection of the ratings could be Excel® spreadsheets, Word forms, email and/or in person interviews. In order to control the effort required to assess the line of business responses, it is recommended that the RIM Risk self-assessments be staggered throughout the year. This scheduling also allows for the accommodation of peak times in the calendar year for certain business areas.

A designated "executive sponsor" must be chosen to provide program oversight and direction and to give you a voice at senior level meetings. Logical sponsors may be your Chief Compliance Officer, Chief Information Governance Officer, Chief Information Officer or someone from their senior staff.

ROLES AND RESPONSIBILITIES

It is important to consider your organization's culture and business structure in order to understand who you, the RIM professional, must collaborate with in order to guarantee the success of your RIM Risk & Control Framework implementation.

Support is needed from the most senior leaders in your institution to emphasize the importance of and expectations for adherence to the program. As such, a designated "executive sponsor" must be chosen to provide program oversight and direction and to give you a voice at senior level meetings. Logical sponsors may be your Chief Compliance Officer, Chief Information Governance Officer, Chief Information Officer or someone from their senior staff.

The following are high-level descriptions of typical primary and secondary RIM Risk & Control assessment roles, along with their responsibilities. Depending on your organization, the roles may have different titles and/or some functions may be combined, such as Legal and Compliance.

You may also opt to use the primary and secondary role responsibilities to identify necessary skills for job descriptions or to help select partners to assist you with your RIM or IG programs.

PRIMARY ROLES:

Executive Sponsor

- Has overall accountability to ensure that the RIM Risk Assessments are conducted across the enterprise
- Obtains buy-in from senior leaders across all lines of business and from the executive suite
- Assists the RIM officer if lines of business do not follow remediation or corrective action plans to ensure compliance

Records and Information Management Officer

- Oversees RIM Risk Assessment program
- Works with lines of business to identify top risks based on loss events or incidents and newly emerging risks
- Acts as subject matter expert in assessing effectiveness of risks and controls
- Creates remediation plans for lines of business that do not meet satisfactory levels of compliance
- Implements corrective actions, plans and solutions to resolve issues
- Establishes an operational structure, processes, controls and reporting required to adhere to the RIM Policy
- Represents lines of business on key corporate information governance committees and working groups
- Ensures lines of business receive Risk Assessment communications and training
- Supports and guides the lines of business on compliance with the RIM program
- Collaborates with partners: Risk Management, Compliance, Audit, IT, etc., to ensure success of the program

Line of Business Manager

- Understands shared goals and responsibilities for developing and executing RIM policies within the business
- Establishes records risk awareness within the business, documents loss events
- Socializes Control guidelines to appropriate areas
- Accurately completes the RIM Risk assessment within the allotted timeframe
- Manages corrective action plans to ensure remediation of Control and risk management gaps
- Establishes governance over line of business records program
- Complies with Global RIM Risk Assessment program
- Collaborates with centralized and/or line of business RIM team, including Record Coordinators

SECONDARY ROLES:

These roles can be chosen to interact with the RIM Risk & Controls Assessment program at various stages of its creation, launch, execution and monitoring. They may make recommendations for modifying how Controls are selected, described and/or ranked based on their specific subject matter expertise understanding of your environment.

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 selection and wording of the Controls deemed appropriate for your organization.

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. This function institutes a repeatable process with associated guidelines to manage the spectrum of simple through complex litigation which impacts the Legal Hold Controls within the Framework.

Risk

The Risk function is responsible for the protection of the organization's brand, finances and operations by managing and mitigating risk exposures. This purview requires a full understanding of the organization's risk profile (litigation, investigations, regulatory requirements, protection of private information, protection of intellectual property, etc.) and associated Controls. It should be closely involved with the RIM Risk & Controls Framework to ensure Controls are accurate and up-to-date.

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, industry groups, etc.). 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. As such, Compliance has vital input to effective RIM Risk Controls for your organization.

Information Technology

The Information Technology function is shifting to be more aligned with lines of business and their objectives. It can provide input for RIM Controls dealing with the proper protection and authentication of data and its availability for use, preservation and disposition.

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 (PII), including medical data and financial information and laws and regulations for the use and safeguarding of consumer financial and banking transactions. This role can be consulted regarding the proper protection and safeguards for specific "high risk" information and its impact on the RIM Controls.

Information Security

The Information Security function is responsible for the development, implementation and management of the organization's security vision, strategy, policy and programs. This function is responsible for policy creation; technology selection and implementation; monitoring and informing parties about malware, breaches, hacking, etc.; and issuing data classification codes (in conjunction with Legal). It should review the security related RIM Controls for accuracy.

Data Officer

The Data Officer function selects, gathers, analyzes and interprets data to increase an organization's efficiency, productivity and revenue. This role requires business skills, technical understanding of computers and data systems and the ability to interpret large amounts of data using data analytic and visualization tools. The Data Officer must work closely with others to ensure compliance with privacy requirements in the use of data beyond its original purpose.

International Representation

Since RIM risk extends across an organization's entire enterprise, there must be proper representation from global functions in the creation, implementation and on-going execution of the RIM Risk & Control Framework. This international representation could be in the form of a delegate from a region (i. e., Asia Pacific, EMEA and North America) that can speak to the concerns of the different jurisdictions within the region.

Human Resources/Internal Communications

Depending on your organizational structure, the Human Resources and/or Internal Communications team can help with properly introducing the RIM Risk program throughout the enterprise, building out training materials, providing advice about delivery mechanisms and translation requirements and ensuring on-going communication about the program.

Metrics for the RIM Risk Controls should be identified, captured and reviewed on an ongoing basis. This consistent data collection approach allows for benchmarking and refinement of your RIM Program, which may enable continued investment and resourcing, as well as to promote greater senior leadership awareness and adoption of RIM and Information Governance.

MEASURES OF SUCCESS

Line of business compliance with RIM policies and procedures must be monitored and reported to senior management and discussed in the appropriate risk or governance forum.

Some examples of measures for a successful RIM Risk & Controls Framework are:

- Improved line of business ratings year over year
- Improved organizational Key Performance and Risk Indicators as a result of greater compliance to policy
- Increased employee awareness of RIM policy and requirements
- Lack of regulatory criticism
- Avoidance of damage to your brand

Metrics for the RIM Risk Controls should be identified, captured and reviewed on an ongoing basis. This consistent data collection approach allows for benchmarking and refinement of your RIM Program, which may enable continued investment and resourcing, as well as to promote greater senior leadership awareness and adoption of RIM and Information Governance.

We encourage you to modify and expand on the list above given your organization's unique abilities and methods for gathering and analyzing data.

ACTION PLAN FOR IMPROVEMENT

The first step in improving your RIM Risk profile is to use the ratings to assess how your organization measures up. Once you have determined your self-assessment scores, there may be a need to create an action plan to improve the overall RIM Risk score or the score of an individual control in particular.

ASK YOURSELF:

Which of the Risks pose the greatest threat to your organization and which of the controls must be enhanced immediately to close off any clear gaps for those risks?

Determining the order of priority for remediation will help you to craft a plan that is focused on critical areas. Moving from a "two" rating to a "one" rating might not be as critical to your institution as moving from a "three" to a "two" for certain risks.

Can the RIM team alone institute changes to enhance the controls or is a partnership with another functional area required?

For example, the RIM team alone can enhance inventory tracking and reporting, but would likely have to work together with Legal and Compliance to make enhancements to the Legal Hold controls. Think about what partnerships might be required and how to secure buy-in from those partners.

What resources are required to enhance the controls?

You may need to ensure that there is sufficient budget for a new or enhanced inventory tracking system if the current one does not provide the level of control needed to track the inventory properly. Or you may decide to hire external subject matter experts to help you construct a roadmap to reduce overall risk.

What is the cost/benefit ratio for the enhancements?

Determine whether the time, effort and cost of enhancing a Risk Control is worth the outcome to make sure you are focused on achievable results.

A well thought out action plan lays out not only the remediation steps and the resources needed to achieve them, but also takes into account the key benefits to the organization and demonstrates clear outcomes. Keeping the plan focused on what is achievable and realistic given your institution's risk and control framework allows you to show measurable success over time.

CONCLUSION

Lately, every professional association and analyst survey or benchmark report that measures the health of Records and Information Management (RIM) or Information Governance (IG) programs comes to the same conclusion: organizations have invested in RIM programs (95% of companies with more than 2,500 employees per the Cohasset/ARMA Benchmark Survey) yet only a handful can be confident that their lines of business are compliant with all aspects of RIM policy.

The burden of monitoring compliance has outgrown the capabilities of RIM staff; there is too much information created every day in myriad business units around the globe, the majority of it by technology, for them to be confident about its management. While this is true for all industries, it is especially problematic for highly-regulated industries because of the significant demands and scrutiny that you face.

The most pragmatic solution to the challenge of measuring compliance is to engage the lines of business in a self-assessment exercise. The RIM Risk & Control Framework presented in this guide suggests a set of RIM Controls that can be standardized to suit your organization's risk profile for distribution to all of your lines of business. With guidance and instruction from your RIM team, line of business managers must represent their ability to satisfy a control by ranking themselves. While the tendency may be to overstate one's capabilities, the respondents should be encouraged to be as accurate as possible to allow for remediation, with no repercussions, unless an egregious violation to policy is reported.

Take advantage of this guide to:

- Institute the Framework as a self-rating tool
- Use resulting RIM Risk scores to rate lines of businesses and geographies
- Reconcile Controls with or map to, any existing corporate controls
- Act as a second line of defense when working with both internal and external authorities
- Update RIM Policy
- Supplement key awareness sessions regarding audits

Lastly, once adopted, publish the Practical Guide for an RIM Risk & Control Framework on your corporate RIM intranet as a resource for all to access.

More Resources

For more information about Information Governance and Metrics, please see A Practical Guide to Information Governance and A Records and Information Managers' Guide to Assessing Performance Risk.

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.