

TRUTH OR DARE: CAN YOU PROVE COMPLIANCE?

Insert Presenter Name



AGENDA

Drivers

Describe the Framework

Review Controls

Implementation Advice

- Oversight & Delivery
- Measures of Success
- Plans for Improvement

Your Compass for Action



▶ **Have you
experienced**

THE GAP?



There's you... and your team



CHALLENGES

Multiple business units, geographies,
regulatory & operational requirements...

and all of this!

THE RIM RISK FRAMEWORK

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

RETENTION

Retention is the foundational requirement of managing records, in any format, digitalization of records to enable assignment of retention rules.

CONTROL	DESCRIPTION	SUPPORT
Records Retention Schedule	A Records Retention Schedule supports compliant management and classification of records across all formats, LCRs 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.	<ul style="list-style-type: none"> - A centralized, enterprise Retention Schedule is created by legal research, subject matter experts and operational requirements and reviewed. - Legal research for each and reviewed on a regular basis. - A process exists to handle changes to the Retention Schedules. - A reportable audit trail exists for Retention Schedules.
Scheduled Review / Active Event	There must be a scheduled review of physical and electronic records to determine lifecycle stage and appropriate retention management action: deletion, archive, and/or 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.	<ul style="list-style-type: none"> - Each LCR conducts a review of records. - Inactive records are expected to take part in the storage, preservation, and disposal process. - Employees are expected to follow the instructions for the disposal of their records.

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 "ongoing effort 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."

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.

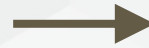
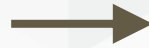
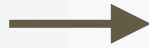


Only 7% report employees are engaged in RIM.

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

A PRACTICAL GUIDE Risk & Control Framework

Establish an operational self-assessment program



1

Institutionalize
a consistent
protocol for all
to use

2

Allow business
managers to
diagnose their
performance

3

Identify and
address
weaknesses in
RIM processes

4

Provide
evidence of
compliance
to authorities

Functions

RIM

Risk + Control



TRAINING	GOVERNANCE	INVENTORY
STAFFING	RETENTION	DISPOSITION
VENDOR MANAGEMENT	PRIVACY & SECURITY	LEGAL HOLDS

Establish a consistent rating scale for all controls

COMMUNICATE
Purpose & Process



DISPOSITION

CONTROL	DESCRIPTION	SUPPORTING INFO	RATING
Secure Destruction of Eligible Records	Records eligible for destruction are securely disposed of in accordance with RIM Policy and Information Security protocols.	<p>Roles and responsibilities of the secure disposition process are clearly defined and communicated in policy and procedure.</p> <p>Electronic data or physical record secure destruction standards are upheld consistently and audited.</p>	<ol style="list-style-type: none"><li data-bbox="1168 216 1839 317">1 All eligible records are disposed of routinely and securely. The process is documented and regularly audited.<li data-bbox="1168 336 1839 437">2 Eligible records are disposed of securely, but the process is not audited or discrepancies have been found in the process.<li data-bbox="1168 456 1839 558">3 Some, but not all, eligible records are securely destroyed or there is no confirmation in writing of the secure destruction.<li data-bbox="1168 576 1839 678">4 Records are not disposed of in a secure manner.

INVENTORY

CONTROL	DESCRIPTION	SUPPORTING INFO	RATING
Line of Business (LOB) Records Indexing	<p>Taking guidance from the RIM team, each LOB must develop a records index in sufficient detail as 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.</p>	<p>LOB indexing reflects the use of the appropriate record code/record class from the company retention schedule.</p> <p>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. .</p>	<ol style="list-style-type: none"><li data-bbox="1168 216 1837 489">1 LOB maintains complete and accurate indexing of all records & can respond to Legal Hold notices, or requests to produce information, in a timely and efficient manner. Performs self-audit at least annually to reconcile vendor indexing with LOB indexing of physical records. Changes made to Schedules are updated accordingly.<li data-bbox="1168 503 1837 642">2 LOB maintains an index of records but it is not fully complete, accurate or updated periodically to reflect changes to the Schedule.<li data-bbox="1168 656 1837 827">3 LOB maintains 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 Schedule.<li data-bbox="1168 841 1837 958">4 LOB does not maintain any index other than what is in physical records vendor tracking inventories and/or data maps.

IMPLEMENTATION

Your Involvement

- Initiate & collaborate in selection of controls
- Provide input into collection method
- Communicate purpose & practice to lines of business
- Conduct a pilot



Take a
Leading Role

Establish a formal process for review and maintenance

○ ANNUALLY

- Identify new risks, add or modify controls
- Confirm applicability of current controls, edit as required
- Review input from LOBs re ease of use, rating system, etc.
- Make appropriate changes to process & communicate to LOBs
- Monitor methodology
- Engage any new stakeholders

○ QUARTERLY

- Assess how controls are functioning
- Recommend changes to oversight team & communicate to LOBs

○ CONTINUOUSLY

- Identify gaps in Framework design & execution
- Receive input from LOBs
- Recommend changes, as required

Method of delivery

Provide evidence of submission

USE TECHNOLOGY

- Survey tool
- Dashboards

OTHER OPTIONS

- Excel Spreadsheets
- Word or PDF forms
- In-Person interviews

Roles and responsibilities



Measures of success



Identify, capture,
and review on an
on-going basis

- Improved LOB ratings year-over-year
- KPI & KRI improvements
- Increased employee awareness of RIM policy and requirements
- Lack of regulatory criticism
- Improved audit results
- Avoidance of damage to your brand

Action plan for improvement

Which risks pose the greatest threat to your organization and which controls must be enhanced immediately to close off gaps?

What resources are required to enhance the controls?

What is the cost/benefit ratio for the enhancements?

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

1

2

3

4



Move the scale

Use the ratings to assess how you measure up

ACTION ITEMS

Your Compass



Leverage
the guide

Promote
the
Framework

Align
with
Partners

Select
appropriate
controls

Pilot
the self-
assessment
process

Use
results to
gain support

▶ **Celebrate your success!**



IRON MOUNTAIN[®]

INFORMATION IS EVERYTHING

To obtain a free copy of the
Practical Guide For a Risk & Control Framework please visit:

ironmountain.com/thoughtleadership

1.800.899.4766 (IRON)