IRON MOUNTAIN®

A PRACTICAL GUIDE TO RECORDS AND INFORMATION MANAGEMENT DESTRUCTION

WHY READ THIS GUIDE?

Though sometimes thought as an optional "last step" in controlling and managing records and information, the systematic destruction of physical and electronic records is essential to achieving compliant Information Lifecycle Management (ILM). Without it, you cannot ensure your organization is adhering to internal, industry and legislative standards and regulations.

This Guide is a compilation of considerations and practices, based on the experiences of a sub-set of the Customer Advisory Board (CAB) members, for the development of a consistent, repeatable process to destroy records that have met retention requirements and do not need to be held for legal purposes. As you move through the Guide, you will encounter common challenges, considerations and recommendations pertaining to the destruction of records and its relation to compliant ILM. The suggestions contained within have proved successful for financial organizations and are supported by relevant case studies*.

It is important to note, however, ILM programs differ from organization to organization, and the decision to adopt a course of action must be taken in regards to your own situation. For that reason, the Guide does not discuss "defensible" destruction, as the interpretation of "defensible" is determined by your own organization's policy, procedures and legal guidance, nor does it address the disposition of information (i.e., what to do with it at a given point in time).

Routine destruction of records is a common and persistent issue for the majority of organizations. A recent Cohasset/ARMA Information Governance Survey (underwritten by Iron Mountain) reports that 76% of organizations have a "keep everything" culture—which is exactly the same number reported 3 years prior. As more records are created every day, managing their eventual end of life becomes increasingly complex.

INDUSTRY FACT

76% OF ORGANIZATIONS HAVE A "KEEP EVERYTHING" CULTURE—WHICH IS EXACTLY THE SAME NUMBER REPORTED 3 YEARS PRIOR.

INTRODUCTION

WHY DESTROY?

Information Lifecycle Management programs are healthier and more compliant when you destroy what is no longer needed for several reasons, including:

REDUCED RISK:

- less chance of exposure of Intellectual Property (IP) or Personally Identifiable Information (PII) through breach or loss
- compliance with the General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA) of 2018 and other privacy law requirements
- less data or "noise" interfering with meaningful analytics, Machine Learning (ML) and Artificial Intelligence (AI)
- less chance of being sanctioned by the regulators for not following your Records Retention Schedule and/or Records and Information Management RIM) policies

INCREASED EFFICIENCIES:

- less need to spend money searching for responsive records for e-discovery and audits
- reduced storage costs
- greater support for key business activities such as mergers, acquisitions and divestitures; real estate consolidations; internal organizational changes and paper-free or paper-light initiatives

> THE PACE OF RECORDS CREATION WILL NOT SLOW DOWN. KEEPING RECORDS (AND ANY COPIES) BEYOND THEIR REQUIRED RETENTION PERIOD IS A PRACTICE THAT IS UNNECESSARY, INEFFICIENT AND POTENTIALLY DANGEROUS FOR ORGANIZATIONS!

GUIDE TO DESTRUCTION

CHALLENGES WITH DESTRUCTION

Many organizations have difficulty destroying records, and the underlying factors are almost universally rooted in one—or a combination of—the following:

- Not knowing where to start
  - no clear understanding or documentation of risks and constraints
  - no valid Records Retention Schedule that indicates when it is permissible to destroy
- Ill-defined process or execution plan
  - too many people involved in an authorization process
  - no designated authority for approval to destroy
  - no time constraints given for business function review of records eligible for destruction
  - not knowing how to destroy records (paper or electronic) securely
  - no budgeting for destruction
- Legal and operational considerations
  - thinking that a record may be needed someday (for litigation or other reasons) and keeping it longer than necessary
  - changes to laws, rules and regulations
  - poorly managed legal or other holds
- Limited technology
- Missing or inadequate controls

Additionally, there are instances in which records stored in cartons, shared drives, abandoned Share Point sites and other repositories do not have sufficient metadata—that is data that tells what the content is and the characteristics it possesses (e.g., Record Owner, Document Type, Dates, Legal Holds and other associated values)—to determine their context in order to make a decision to destroy. This category of records is often referred to as "orphans" or "unclaimed," and are often retained far beyond when they reasonably should be, simply because no one in the organization knows how to appropriately manage them.

COMMON PRACTICES

CREATE A METADATA STANDARD

In instances where no metadata is attached to physical or electronic records, making a decision to keep or destroy is virtually impossible—regardless of organizational buy-in or want-to. Therefore, if your organization has not yet defined a metadata standard, you must start there. The Customer Advisory Board's Metadata Standard Guide provides a starting point as well as implementation advice.

ESTABLISH AND MAINTAIN A RECORDS RETENTION SCHEDULE

A Records Retention Schedule is a policy document that defines the legal and operational requirements for the length of time records must be retained. Along with metadata (such as when a record is created) it is critical in the determination of when records become eligible for destruction.

DOCUMENT AND DEVELOP A DESTRUCTION PROCESS

A destruction process details the steps taken to destroy records. To be compliant with Records and Information Management policy, it must provide a framework for destroying both physical and electronic records.

The development and approval of a repeatable and approved destruction process is a collaborative exercise that should include IT, Legal, Records and Information Management (RIM), Audit or others depending on your organization. Key business units should be asked for their input, particularly those with records of high risk, value and/or volume. An enterprise-wide, universally adopted destruction process only becomes a reality if all key stakeholders are involved in its development and implementation.

Accountability for records destruction, including the documentation and preservation of all destruction decisions, must be assigned either to an individual, for example someone in Legal or on the RIM team, or a group of individuals spanning different functions, and should be supported by senior staff. More information on the various stakeholders involved in the original and ongoing definition, approval and execution of the policy are described in the Roles and Responsibilities section of this Guide.

Lastly, consistent execution of the destruction process is essential; inconsistent application may put your organization's reputation at risk or subject it to regulatory criticism. If participation lags from a particular business unit, you must put measures in place to ensure timely responses from destruction reviewers or approvers. If a business unit consistently fails to cooperate, escalation to overseeing senior staff is an option to change behaviors. The development of Key Risk Indicators (KRIs) or other metrics for review by business line executives can demonstrate the performance of reporting entities, highlighting areas that consistently retain records beyond their retention period requirements.

VALIDATE AND IMPLEMENT

Pilot programs to test the destruction process and gain user buy-in are a best practice. Once the process is fully vetted and adjustments made, a launch plan for implementation of the destruction process should be created to document roles and responsibilities (more on that later), as well as timing. You should plan to conduct awareness training for business units.

MANAGE VENDORS

In some instances, you may rely on a third party to execute the destruction of your physical and electronic records. Make certain that your requirements are carefully described in your service level agreements (SLA). The SLAs should include some form of certification that destruction was carried out. You will need to monitor the vendor's performance on a consistent basis to ensure that destructions are being completed within the stated time frames.

MONITOR AND ADJUST

The destruction process should be robust and inclusive enough to meet current needs and flexible enough to adjust to future needs. The process should be audited periodically and any gaps identified and fixed. Business units should be monitored for their ability to adhere to the destruction schedule. Test results may indicate that additional or expanded training is necessary to advance employee understanding of the destruction process and policy.

ENSURE THERE IS A DOCUMENTED HOLD PROCESS

A robust record hold process that outlines steps to be taken when the destruction of records is temporarily suspended due to a legal or other type of hold is vital for the execution of a compliant Records and Information Management program.

APPROACHES FOR MEDIA DESTRUCTION: PHYSICAL VS ELECTRONIC

As mentioned earlier, the timely destruction of records is dependent on retention rules (published in a Records Retention Schedule) which apply to both physical and electronic records. The execution of destruction varies based on the type of media, as addressed in this section.

PHYSICAL

The destruction of physical records in a timely and consistent manner can be conducted by either employees or a third-party supplier or both. Whatever your choice, it must be executed according to an approved destruction process.

On a routine basis, lists indicating records eligible for destruction should be generated in-house or by a third-party supplier. The determination of eligibility may be computed by an application (e.g., using the record creation date and retention rule) or manually input at some point during the time of storage, ideally when sent to storage. The documented destruction process should identify to whom the eligibility list is distributed as well as describe the requisite steps leading to the eventual secure destruction of records, onsite or offsite.

Destruction eligibility lists can be generated to project which records are eligible in future time periods in order to plan and budget for destruction events.

For records housed onsite by the business, the business should be made formally responsible in the destruction process for periodically reviewing the files held and destroying them according to the Records Retention Schedule.

ELECTRONIC

To enable compliance with the destruction process for electronic records, a systematic approach to the review of an organization's business applications, including those linked to databases and storage repositories that host digital data, is highly recommended. Applications should be assessed based on their risk or value; factors include vital business functions, applications housing PII or intellectual property and large volumes of data or records – then assigned a priority to facilitate the review.

The following are recommendations for understanding and enabling destruction, dependent on the capabilities of applications.

- Review each application to determine if it is a record-keeping application and what type(s) of records it contains.
- Refer to your approved Records Retention Schedule to assign an existing record code to the application. If there is more than one type of record in an application with differing retention requirements, a common approach is to assign the longest rule to the application. Alternatively, specific rules could be applied to the different record types if the application supports that capability. Decisions about rule assignment should include RIM, the business owner and IT application administrator, with input from Legal and Compliance.

- If during the assessment you discover a record type or class that does not appear in the Records Retention Schedule, follow your established maintenance process to update the Schedule.
- Include information about each application and the types of data associated with it on a business file plan or records inventory. As with a physical records inventory, this inventory of digital records provides an accounting of what you have, where it lives and how long it must be kept, in addition to identification of business and application administrators.

Most information in an organization is considered a record, and each application that stores records must conform to records and information lifecycle management controls. If business units decide to keep records longer than the designated retention period—legitimate reasons include use in data analytics, trending, machine learning or AI purposes, or for their historical value to the organization—they should request a review with the RIM and IT teams to determine where and how long they should be kept. Keep in mind, data separate from a record should be kept only as long as relevant and defined in a control process. The Privacy or Information Security function may require that customer information be masked or de-identified if data is to be retained longer than required for its original purpose.

In the event servers are decommissioned, it is essential to work with IT to ensure that all data is either archived (if the data constitutes "records") or destroyed (if the data are not records). The servers, and any associated hardware, must be securely destroyed and new applications should include records and information management controls to ensure future records are managed per your organization's ILM guidelines.

Finally, auto-destruction (i.e., setting up applications so that records are automatically destroyed without a final review by the record owner based on certain parameters such as creation date and retention period of the record class) of electronic records should never be conducted without prior alignment with litigation team requirements, as you may need to satisfy litigation or audit requirements such as litigation holds.

ROLES AND RESPONSIBILITES

It is important to consider an organization's culture and business structure in order to understand with whom the RIM professional must collaborate in order to establish and implement an enterprise-wide destruction process for physical and electronic records.

The following are high level descriptions of the roles most likely involved in the destruction processing decision-making and authorization process, along with their respective responsibilities. Depending on the specific organizational structure, the roles may have different titles and/or some functions may be combined, such as Legal and Compliance.

RECORDS AND INFORMATION MANAGEMENT (RIM)

The RIM function provides policy, governance and consultation for ILM program users, making the function vital to the execution of destruction. Duties include:

- working with vendors and/or internal partners to generate reports of cartons or files eligible for destruction
- working with IT to ensure that scheduled destruction of records in applications with assigned retention rules happens on a consistent basis.

The RIM role typically monitors the process from beginning to end, making sure the business unit owners, Legal or other stakeholders remain accountable for decision-making.

INFORMATION TECHNOLOGY (IT)

Information Technology is expected to efficiently manage the high volume of data being created and received while minimizing costs, particularly around redundant data storage. As such, they are a key stakeholder in the destruction of digital records. They should help to ensure retention rules are assigned to applications by the business owner and execute destruction orders.

LEGAL/RISK

Legal and/or Risk is responsible for determining the risk profile of an organization based on litigation exposures, international privacy requirements, intellectual property protection, working environment and more. Legal should be a party to the development, approval and execution of the organization's destruction policy and process.

COMPLIANCE

Compliance 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.) Compliance should confirm that the destruction process is sufficient to enable compliance to the organization's information governance framework and associated policies, such as the Records Retention Schedule and General Data Protection Regulation (GDPR).

DATA MANAGEMENT OR DATA GOVERNANCE

The goal of the Data Management or Data Governance function is to assist lines of business in ensuring a consistent and controlled approach to the development, use and management of enterprise information assets and critical data elements across an organization, including its destruction. This function may conduct data management practice assessments through various tools such as the Data Maturity Model, Data Quality platform and Data Standards implementation plans.

INFORMATION PRIVACY (IP)

The Information Privacy function is responsible for managing the risks and business impacts of privacy laws, consumer finance laws and policies and responding to regulator and consumer concerns over the use of PII, including medical data and financial information. This role must have input into the creation and execution of the destruction process for the compliant lifecycle management of private and sensitive information.

INFORMATION SECURITY (IS)

Information Security is responsible for the development, implementation and management of the organization's information security vision, strategy, policy and programs. It is responsible for policy creation; technology selection and standards; monitoring and informing parties about data breaches; communicating information security policies and procedures to the business; enabling security standards dictated by customers, such as the government; determining data classification codes (in conjunction with Legal); and remaining compliant with ISO standards and regulatory requirements. Since destruction of data is a key component in enabling its secure management, the IS function should have input into the development of the destruction process.

AUDIT

The Audit function requires quick and accurate access to information for internal or external purposes. The role's inclusion in the development of a destruction process can help facilitate Audit's ability to respond to requests for information.

BUSINESS (OPERATIONS)

The Business (lines of business, business units and/or departments) is ultimately responsible for compliance with the information governance, RIM and information lifecycle policies – including destruction. They are a primary contributor in the destruction review process. Since they own the records in question, ultimate responsibility for ensuring a sound destruction process falls to them.

CONCLUSION

Many organizations believe the benefits of keeping records indefinitely outweigh the expense and effort of developing and managing a consistent, repeatable process to destroy records. But this "keep everything" culture brings significant potential for inefficiencies, high litigation discovery costs, data loss and compliance violations. Destroying records that have met retention requirements and which do not need to be held for legal purposes is essential in ensuring your organization is protecting information privacy and remaining compliant.

Below are links to other resources mentioned in this Guide, followed by a glossary containing definitions of key words. The Appendix features real-world cases studies of financial institutions that have moved beyond a "keep everything" culture, from which you can draw inspiration. It also includes experiences with planned and unplanned incidents or events—such as a real estate move or an unexpected disaster. While some of the situations were unavoidable, the burden of managing through them could have been less onerous and risk-prone if a formal destruction process had been in place.

PLEASE VISIT IRONMOUNTAIN.COM/CAB TO VIEW ALL OF THE CUSTOMER ADVISORY BOARD GUIDES

GLOSSARY

ACTIVE RECORD:
Records related to current or in-process activities. These records are referred to on a regular basis to address internal and external business requirements. For records with event-driven retentions, the event trigger has not yet occurred.

CLASSIFICATION:
The process of identifying and arranging records into categories according to logically structured conventions, methods and procedural rules.

CONTROL:
A standard of performance that has been designated as critical to the disposition process.

DESTRUCTION:
The act of permanently disposing of records. For hardcopy (paper) records, destruction typically involves shredding, pulping or recycling. For digital records, destruction typically involves overwriting data such that the original data can no longer be accessed.

DISPOSITION:
A range of processes associated with implementing records retention, destruction or transfer decisions which are documented by disposition authorities.

ELECTRONIC RECORD:
Records that are communicated and maintained by means of electronic equipment. Also known as digital records.

INFORMATION GOVERNANCE (IG):
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 lifecycle of information, including defensible destruction.

INACTIVE RECORD:
Records related to closed, completed or concluded activities. These records are not routinely referenced but are required to be maintained for legal, regulatory or business reasons. Typically, they are records for which the trigger event has occurred.

INFORMATION GOVERNANCE PROGRAM:
The policies, procedures, processes and controls implemented to manage information.

INFORMATION LIFECYCLE MANAGEMENT (ILM):
A strategy recognizing that the risk, usage and value of information changes over time and must be managed accordingly. ILM seeks to classify information according to its business value and risk factors, establish policies to store it and destroy it appropriately.

INFORMATION PRIVACY:
The obligation of an organization to identify and protect PII and other private or sensitive data.

LEGAL HOLD:
The procedure used to suspend temporarily the normal retention requirements of certain groups of records, even if they are eligible for destruction, due to pending or active litigation.

LIFECYCLE:
The stages of a record or information, which typically include creation, use, maintenance, storage and destruction.

METADATA:
Data that describes data such as the context, content and structure of records and information and their management through time.

MIGRATION:
The act of moving data or records in electronic form from one hardware or software system or one configuration to another so that they may continue to be understandable and usable for as long as they are needed.

NATIVE METADATA:
Metadata created automatically by an application.

NON-RECORDS:
Records that are not required to be retained for business or legal reasons. These may include duplicates or "convenience" copies of Official Records that have not been annotated and may be destroyed when no longer referenced.

ORPHAN RECORDS:
Records that lack the primary metadata (e.g., record code, ownership, description, etc.) necessary to identify and make a destruction decision. Also known as unclaimed records.

PERSONAL IDENTIFYING INFORMATION (PII):
Information that personally identifies an individual and is not otherwise available to the public. Examples include: full name (if not common); home address; email address (if private); national identification number; passport number; IP address (when linked, but not PII by itself in US); vehicle registration plate number; driver's license number; face, fingerprints, or handwriting; credit card numbers

UNCLAIMED:
See Orphan Records.

APPENDIX: USE CASES

The following use cases highlight various aspects of the destruction of records, both managed and unplanned. They address how real estate consolidation activities can be triggers for addressing the permanent removal of records and describe formal projects for handling records with little or no metadata. They also reveal how to address unintentional records destruction or damage. Each use case describes the challenge, the solution and lessons learned.

USE CASE STUDY #1: RECORDS MANAGEMENT AND DESTRUCTION DURING REAL ESTATE CONSOLIDATION

DESCRIPTION OF ORGANIZATION

A Fortune 500 worldwide financial services company with over 30,000 employees. The second-oldest financial institution in the US, operating in more than 29 countries.

CHALLENGE

While restructuring its real estate footprint, the organization discovered its information destruction policy had not been updated and modernized in several years, leaving hundreds of employees wondering what could be kept and what could be destroyed. In many cases, the Real Estate team was surprised by desk drawers, cabinets and conference rooms full of ownerless records that had accumulated over decades. These records needed to be addressed, as the new employee work space had no room for onsite paper file storage.

SOLUTION

A multi-departmental approach was developed to establish a defensible destruction policy. Involving Real Estate, Compliance and Procurement, the company developed a set of guidelines for what records needed to be kept and what could be destroyed. An onsite resource from a chosen destruction / storage partner was assigned to work side-by-side with Facilities Management as they worked on the floorplans for each building being de-fitted. This resource identified each group of records and connected them with the owner (or owning business unit). The onsite resource then worked with the owners to assign a retention profile and send records to storage or securely destroy them if the retention period was met and no legal hold was in place. Records in non-paper formats (such as thumb drives) were addressed in the same manner.

The processes provided a painless introduction to information destruction and allowed for a more effective adoption of the new "clean desk" policy in place in the new work environment. The relationships and credibility established in the destruction process allowed for high levels of end-user engagement, no records being left as "unidentified," a reduction in corporate risk through the destruction of thousands of old records that were past their retention requirements and the establishment of a the defensible foundation for a routine destruction program for all employees.

LESSONS LEARNED:

It is crucial to start the communication process as early as possible when moving facilities. It's also vital to have involvement from not just Real Estate, but Compliance, Procurement, the Business record owners and the destruction / storage vendor. Tangible benefits can be achieved for each of these groups if a destruction policy is established using the building move as the initiating event.

- Compliance establishes a destruction process and reduces risk
- Real Estate can hit their target move date
- Procurement can avoid the costs to move or store unnecessary records
- The business needs to make the decisions about the records.

USE CASE STUDY #2: UNCLASSIFIED RECORDS OWNERSHIP AND DISPOSITION PROJECTS

DESCRIPTION OF ORGANIZATION

An international financial institution headquartered in the US with over 280,000 employees operating in more than 40 countries.

CHALLENGE

The financial institution needed to ensure all records stored offsite had line of business owners responsible for their classification, retention and disposition. This exercise included records in offsite storage where ownership was not clearly specified in the account structure hierarchy or where ownership had been declined by business units previously identified as likely record owners.

SOLUTION

Major stakeholders, including representatives from major lines of business, were brought together to remediate the situation. They classified records according to the following process:

- developed a three-level enterprise account ownership hierarchy (based on Iron Mountain's "Customer ID/Division ID/Department ID" fields in SafeKeeper Plus)
- assigned separate Customer ID numbers to each major line of business (e.g., Community Banking, Consumer Lending, etc.)
- assigned more granular division and department identification codes, based on organizational structure
- generated a variety of review reports; used an "iterative" approach involving multiple review rounds to identify ownership
- worked with stakeholders (group records coordinators, records coordinators and subject matter experts) to formalize ownership, using this account structure hierarchy
- for those records for which stakeholders claimed ownership, transferred those records into the appropriate Account ID/Division ID/Department ID structure
- for those records that remained "unclaimed," created a separate Customer ID number and moved these records into this new Customer ID

At the end of this project, organizational ownership was assigned to all records and the organization had a process to ensure the timely review and disposition of unclaimed records. Now, no new records can be transferred into this separate Customer ID unless they are records acquired through acquisitions but are not claimed by existing business units. These records are classified to the Records Retention Schedule and destroyed or retained accordingly. At some point in the not too distant future, the organization expects this "unclaimed" Customer ID will contain no records and can be closed.

LESSONS LEARNED:

- Departments to which the records had been assigned were not always accurate due to enterprise reorganizations.
- As additional reorganizations take place, all affected boxes must be moved into any new organizational structure.
- Inventory must be monitored on an on-going basis to ensure accurate ownership assignment.

As a result of these lessons learned, the organization marked certain fields as "required" when users send inventory to storage to prevent the transfer of boxes into invalid divisions and departments.

USE CASE #3: ADDRESSING UNINTENTIONAL RECORDS DESTRUCTION AND DAMAGE

Though never ideal, unintentional records destruction and/or damage does present an opportunity to reevaluate and improve records and information management, including storage and destruction policies and procedures. In the following pages, we examine common scenarios, best practices following unexpected destruction and/or damage, recommendations to mitigate future risk, as well as uses cases demonstrating how various financial institutions dealt with but also capitalized on the unexpected.

Examples of unintentional records destruction/damage scenarios include:

- Natural disaster
- Isolated fire, flood/water damage, collapse, etc.
- Infestation/mold
- Improper/premature destruction (protocol breach/miscommunication/misunderstanding)
- Lost or misplaced records

In these instances, the following remediation steps should occur.

1. Control the scene.
2. Take stock of what was damaged/destroyed/lost.
3. Determine what can be recovered. Engage remediation/recovery service as applicable.
4. Document the original scenario, its root cause, prognosis, and the action/remediation plan.
5. Brief internally (Legal, Compliance, Risk, Privacy, etc.) to determine next steps (is there a need to notify regulators, LOB, customers, etc.?)
6. Proceed with agreed upon plan, documenting and updating stakeholders routinely on progress.
7. Upon close of project, share updates with stakeholders.
8. Update and retain documentation.

To reduce or mitigate the risk of unintended destruction, regardless of scenario, the following are best practices.

1. Instill preventive measures where possible (new policies, procedures, protocols, controls, etc.). Include clauses in contracts to prohibit storage in high risk areas. Ensure vendor contracts have appropriate safeguards and suitable notification provisions/mechanisms.
2. Self and vendor audit of box condition in facilities based on how long something is in storage. Controls put in place to follow trucks and shadow process when recovery by a third party is necessary.
3. Capture onsite records in a business inventory.

USE CASE 3A: WATER DAMAGE FROM FLOODING

DESCRIPTION OF ORGANIZATION

An international financial institution headquartered in the US with more than 50,000 employees operating in more than 35 countries.

CHALLENGE

After a hurricane flooded the bottom floor of one its major buildings and various hardcopy formats – microfilm, microfiche and paper – as well as equipment and office materials were water damaged, the institution had two goals. One, rescue and restore as much of the information as possible, as quickly as possible, while protecting the records from inadvertent disclosure, and two, track down the information owners so they could decide whether to keep, store or destroy their records.

SOLUTION

A remediation vendor who could restore affected records by freeze-drying them was brought in. The vendor catalogued all of the material in the affected areas and placed them in refrigerated trucks to be transported cross-country to a restoration facility. Indexing was done by using any descriptions on the outside of cartons, the notations on film and fiche containers and the number of the room / location from which the material was removed.

In the meantime, the Records Management tracked down the owners of all of the records. Where there were no clear descriptions on the cartons, a site map of the basement was used to determine which businesses were storing records in which rooms of the basement. The owners were then given the listing of records and asked what they wanted to do.

Out of 3,000+ cartons of paper records and four cabinets of microfilm and fiche, all but 325 carton owners were found. These unknown records were "ring fenced," and on the advice of the Legal Department, put into storage for a 10-year period. The store of microfilm and microfiche was moved to a storage vendor's highly secured facility, where there was no chance of environmental damage.

LESSONS LEARNED:

While the vendor was able to restore all of the records and ultimately no information was lost, the situation could have easily turned out differently. As a consequence, the institution expanded its Records Management policy to:

- prohibit storing records onsite in environmentally risky areas
- store microfilm and microfiche in a highly secured facility, with no chance of environmental damage
- require full indexing of records on site to be included in each business' file plans
- require a destruction review for on-site records of at least annually.

Now, as part of their routine examinations, Internal Audit reviews each business against these new standards to ensure compliance with the policy.

USE CASE 3B: FIRE DAMAGE

DESCRIPTION OF ORGANIZATION

An international financial institution headquartered in the US with more than 50,000 employees operating in more than 35 countries.

CHALLENGE

The institution was notified a fire broke out in one of its vendor's hardcopy records storage facilities in the UK. All the company's paper records (approximately 1,000 cartons) in that warehouse were destroyed. The institution thus had to determine:

- exactly which records were lost
- whether duplicate copies of the records existed in another format
- whether notifications to clients and regulators needed to be done

SOLUTION

After the Records Management team alerted senior management and the businesses that owned the records, a task force of representatives from Compliance, Risk, Legal and RIM was quickly put together to gather information about the material in the warehouse.

Unfortunately, the inventory tracking of these cartons in some cases contained only minimal information, such as when the carton went to storage. For approximately half the boxes, the indexing held within the business was robust enough for the team to determine exactly what was lost and which records were held elsewhere digitally. The Compliance team had to notify the regulators of this incident. The institution took steps to enhance protocols around records indexing and vendor risk assessments.

LESSONS LEARNED:

It is critical to have appropriate indexing – both within the hardcopy records tracking system and a more complete version held by the carton owners – in order to support the actions that need to be taken when an unforeseen event destroys company records. Knowing where duplicate copies may be held is also beneficial. Communication with the vendor is key to swiftly getting on top of the situation.

USE CASE 3C: MISSING BOXES IN MIGRATION

DESCRIPTION OF ORGANIZATION

A banking and financial services company headquarters in United States with 55,000 employees across the US, Europe, Canada and Asia.

CHALLENGE

While migrating over 1 million cubic feet of physical records storage from approximately 20 legacy providers to a single provider, the bank discovered most of the legacy contracts were inherited in acquisitions of other banks and much of the content was old and poorly identified.

With the project about 90% complete, only .05% of boxes shown on legacy vendor inventories with "In" status have not been found on legacy supplier shelves. However, almost all of the missing boxes belonged to an acquired bank's Mortgage Lending unit and were on regulatory and legal hold.

SOLUTION

Assuming that high-risk boxes had been accidentally destroyed, were lost in the warehouse or were never on the shelf to begin with was not an option. An investigation uncovered:

- An in-house inventory of boxes sent offsite still existed in the Mortgage Lending business unit. The internal record showed that 105 of the boxes shown in the supplier inventory with "In" status had either been destroyed or permed out.
- A receiving supplier conducted a search of their inventory and found five more boxes that they had initially reported as not received.
- The legacy supplier found 107 more boxes located on their shelves.

The Mortgage Lending business performed another scan of their in-house inventory to determine whether any of the remaining 298 boxes could be found under barcodes other than those listed in the supplier inventory.

The next step was to identify the root causes of inventory discrepancy. Two factors were discovered. One, a shelf collapse at legacy supplier warehouse in 2004 resulted in unreliable repacking of boxes, and two, multiple supplier acquisitions and multiple software changes over the years resulted in unreliable record-keeping.

LESSONS LEARNED:

A failure to properly manage—and audit (!)—inventory can lead to the retention of unknown records or the inability to locate a record directed for destruction.

800.899.IRON | IRONMOUNTAIN.COM

USRM-BP-111318A