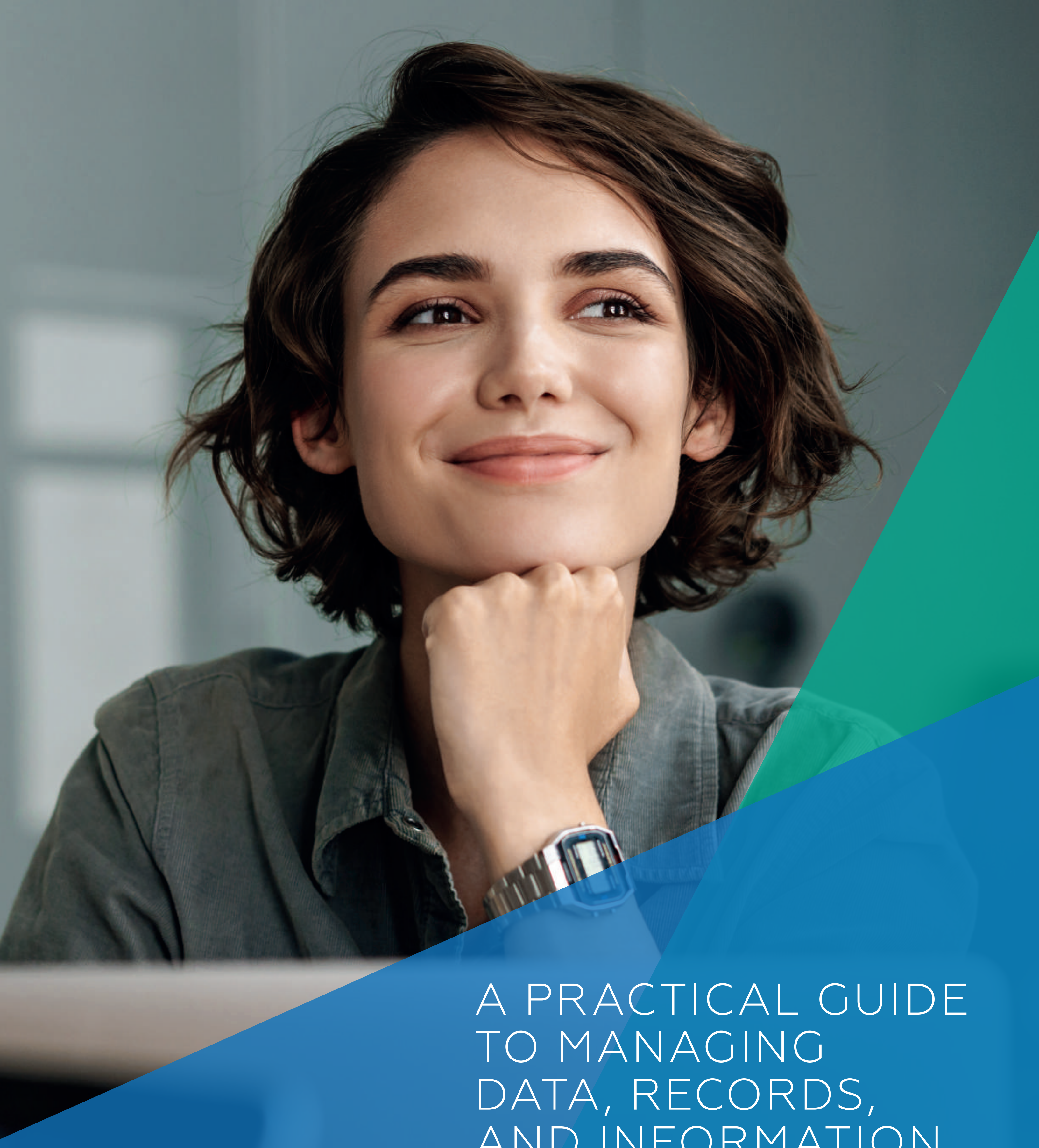


A PRACTICAL GUIDE TO MANAGING DATA, RECORDS, AND INFORMATION

IRON MOUNTAIN®

A PRACTICAL GUIDE TO MANAGING DATA, RECORDS, AND INFORMATION

WHY READ THIS GUIDE

In today's world, the word "data" is a catchall that includes what Information Management professionals know as distinct entities: records, data, and information. While the lines between them are blurred, it is vital that we understand the difference to ensure compliant, secure, and efficient control over, and use of, an organization's records and data.

While this practical guide covers the many reasons why it's critical to fully understand the relationship between data, records, and information, its ultimate purpose is to foster conversations between those providing technical capabilities, namely IT teams, and the organization's users and information managers.

Once understood, the dependencies common to how information is governed—Data Governance (DG) and Information Governance (IG)—can be used as leverage to consolidate efforts to meet enterprise-wide operational and regulatory requirements, including the ultimate disposition of data and records. Remember: there is no "one size fits all" answer to how data and records are managed; it is dependent on the various considerations and obligations of each organization.

*The information in this document is made available solely for informational purposes. No content within this document is intended as legal advice, nor should any content within the document be construed as legal advice. This document presents situations and approaches for dealing with them, and those situations or possible approaches might not apply to your organization. We do not warrant the accuracy, completeness, or usefulness of this information. Any reliance you place on such information is strictly at your own risk. The authors and Iron Mountain disclaim all liability and responsibility arising from reliance placed on such materials by you, or by anyone who may be informed of any of its contents.

INTRODUCTION

WHY NOW?

Records and Information Management (RIM) and IG teams are actively seeking advice for how to create a strategy that aligns data with traditional records and information management programs, including records retention schedules. While many organizations have a clear direction for how long records must be kept before disposition (typically approved by a Legal/Compliance function), there's a lack of clarity about how long data should be retained, and who has the authority to make those decisions.

With the majority of transactions and official records now born and held digitally, rather than on paper, there's an increased need to be data literate. Data privacy and localization laws, use of artificial intelligence (AI) and machine learning (ML), and cybersecurity threats demand that we understand what data is used where, for how long, and when it can be destroyed. In essence, data is input that must be managed—and classified—through every stage of its use.

DEFINITIONS

Before we can have meaningful discussions about the management of data, records, and information, we must first define them. The following are industry recommendations:

DATA:

- Set of characters or symbols to which meaning is or could be assigned. (ISO 30300:2020)
- Any symbols or characters that represent raw facts or figures and form the basis of information. (ARMA: 2016 vetted by ANSI the American National Standards Institute)

RECORD:

- Information created, received, and maintained as evidence and as an asset by an organization or person, in pursuit of legal obligations or in the transaction of a business. (ISO 15489-1:2016)
- Any recorded information, regardless of medium or characteristics, made or received and retained by an organization in pursuance of legal obligations or in the transaction of business. (ARMA: 2016 vetted by ANSI the American National Standards Institute)

INFORMATION:

- Data in context with a particular meaning. (ISO 30300:2020)
- Data that has been given value through analysis, interpretation, or compilation in a meaningful form. (ARMA: 2016 vetted by ANSI the American National Standards Institute)

Data Governance and Information Governance are separate entities or functions, yet by their definitions, have much in common—and technology is their connective tissue.

DATA GOVERNANCE

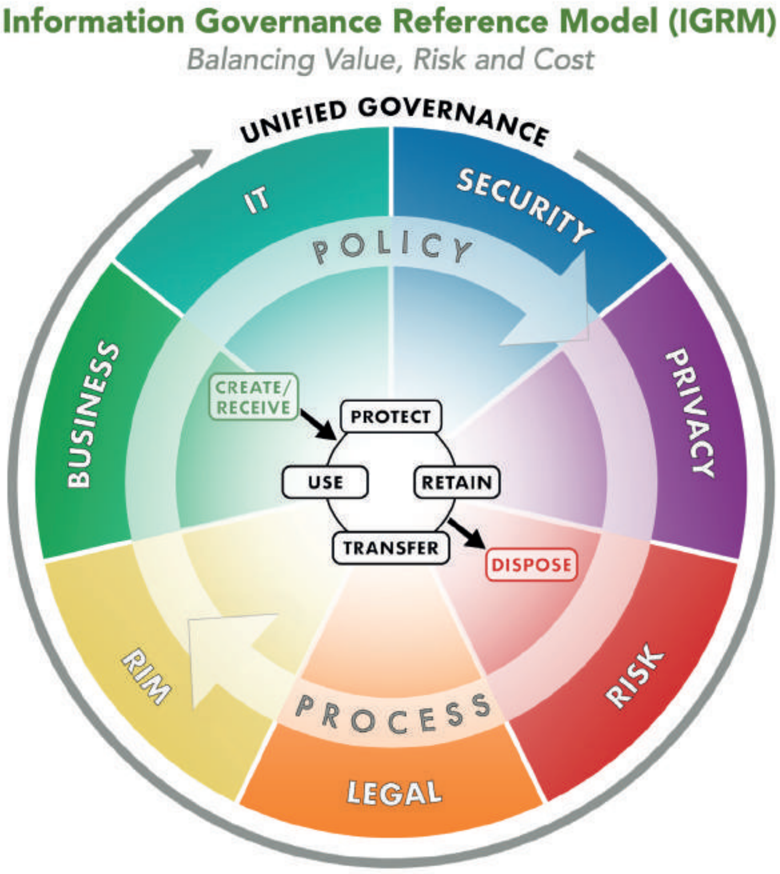
- Policy, processes, practices to address data quality
- Focus on metadata, standards, models
- Technical considerations of data lifecycle
- Led by Chief Data Officer

INFORMATION GOVERNANCE

- Policy, processes, practices, roles, and metrics to manage information through its lifecycle
- Focus on meaning and use of information
- Legal and compliance considerations of information lifecycle
- Led by Chief Information Governance Officer (CIGO) or other executive

Please note, for the purpose of this guide, we address Information Governance as a "concept" rather than a specific "function" within an organization.

The Information Governance Reference Model (IGRM) shown below has been used for over a decade. The framework provides a unified governance approach to information by showing the linkage between value and duty to information assets—whether records or data. This aligns with our use of IG as a concept rather than a function.



Information Governance Reference Model © 2022

DATA, RECORDS, AND INFORMATION: A DEPENDENT RELATIONSHIP

There are many reasons why coordination and collaboration between IG and DG is becoming increasingly urgent. Here are the most prominent:

Data is very often the source for records creation.

Traditionally, the focus of records and information management has been on *output*– the tangible record created or received by an organization for which specific rules, regulations, and controls inform its lifecycle management.

Data elements are pulled from databases as *input* and assembled in prescribed ways to yield reports as *output* essential to an organization's operations. The same data field may be used for multiple reports (e.g., customer id). A useful analogy is to consider data as ingredients such as flour, sugar, and eggs that are called for in recipes to create different end products like cake or bread. Just as the cake has a different "use by date" or retention rule from the bread, once created it's no longer dependent on the source of its components. Similarly, an official record is no longer dependent on the data used; it is created at a particular point in time and re-creation may or may not be possible.

Data, both structured or unstructured, is the ever-increasing target of cybersecurity hacks, breaches, ransomware, and other nefarious activities.

All organizations are vulnerable to attacks on their data. Gartner research warns that cybersecurity threats and ransomware attacks will impact 95% of organizations through 2024. Cybercrime Magazine predicts global ransomware damages to reach USD$42 billion by the end of 2024 after reporting that ransomware will have attacked a business every 11 seconds in the same timeframe.

The reality of this risk requires organizations to protect data, recover quickly from attacks, and make consumers aware of a breach, as dictated by privacy laws, all of which carry a heavy price tag and have consequences for a brand's reputation. These actions require collaboration among a number of stakeholders, including IG and DG professionals, and should lead to strategies that map data, prioritize it based on exposure risk, and determine a plan to get rid of data that is no longer required.

CYBERSECURITY THREATS AND RANSOMWARE ATTACKS WILL IMPACT 95% OF ORGANIZATIONS THROUGH 2024

Persistent changes to and emergence of new regulations to protect private and sensitive information may have increasingly severe consequences for non-compliance.

Data privacy protection laws continue to evolve and expand across the globe. With guarantees for consumers' rights including to be forgotten, to request where data is stored and how it's used, and much more, comes the responsibility for rigorous controls about data and the management of its lifecycle. And increasingly, organizations are being fined for violations to these regulations, such as Canada Bill 64 and the EU's General Data Protection Regulation (GDPR).

This is the domain of no single function in an organization; it takes input from representatives from Legal, Privacy, IT, RIM, IG, DG, Data Officers, Security, and other areas of dependency and importance to achieve maximum compliance.

There is a dependence on data to provide valuable insights gleaned from analytics and AI and ML tools.

Data is the ingredient for innovation, customer satisfaction, R&D, healthcare discoveries, predicting events, and so much more. Many of these uses are within the purview of lines of business, rather than a central function. To be of ultimate value, data sources must be identified and elements must be accurate and authentic. It's important to consider the quality and age of the data before making decisions about its disposition; outcomes are cleaner and quicker when "noise" from redundant, obsolete, and transitory/trivial (ROT) data is removed.

OUTCOMES ARE CLEANER AND QUICKER WHEN "NOISE" FROM REDUNDANT, OBSOLETE, AND TRANSITORY/TRIVIAL (ROT) DATA IS REMOVED

The sheer volume and variety of data from countless sources creates new challenges.

IDC calculates that in 2010 the world created about two zettabytes (ZB) of digital information. If that were put into 1 gigabyte thumb drives that were then laid end to end, it would make a line that could stretch across 184 million football fields. And Forbes asserts that the amount of data created, captured, copied, and consumed in the world increased from 1.2 trillion gigabytes to 59 trillion gigabytes, an almost 5,000% growth from 2010 to 2020. It's obvious that methods of management created for paper, with such a dependence on the human element, cannot scale to meet this tremendous influx of data.

The cloud continues to be selected for essential business operations.

The global pandemic has accelerated the use of cloud-based applications that support collaboration, allow easy access to records via a central repository, provide a consistent user experience for geographically dispersed employees, and more. Data in the cloud must be managed the same as it would be on premises, with special attention given to data localization requirements.

REQUIREMENTS FOR SUCCESSFUL DATA, RECORDS, AND INFORMATION MANAGEMENT

POLICY

We rely on policies to govern how information is compliantly managed throughout its lifecycle. In addition, organizations create "controls" that enable oversight and performance measurement, while some also incorporate standards established by various professional or industry associations.

A records retention schedule is an essential policy that indicates how long records should be retained, after which, with proper authorization, they should be disposed of in compliance with rules and regulations to avoid fines and/or sanctions. Some organizations have begun to "right size" this schedule to include data, along with its emerging requirements related to privacy and data localization rules.

The objective is to represent both the information inputs (data) and outputs (records) that an organization creates and receives in a comprehensive schedule as it moves through all phases of its lifecycle.

APPLICATIONS

With the vast majority of data, records, and information created digitally in cloud-based or on-premises applications, the selection of technology, as well as its use and management, requires strategic collaboration among the stakeholders described in the Roles and Responsibilities section of this guide. The resulting collaboration should yield policy, procedures, and processes that enable execution of data and information governance requirements for all functions.

OVERSIGHT

Accountability is critical for the successful governance of information. Oversight to meet regulatory demands and internal controls must include both records and data. Reporting and escalation models apply for all forms of information critical to risk management.

DISPOSITION

Disposition of information once it has met its legal or operational retention requirement is a necessary activity of lifecycle management. This may mean its secure destruction, transfer to a corporate archive, or movement to a data lake or repository for future analysis or AI/ML activities. Once again, this decision should not be the domain of a single function—value may be found in the information beyond its primary purpose.

ROLES AND RESPONSIBILITIES

As stated at the beginning of this guide, while organizations have a clear direction for how long records must be kept before disposition, there is a lack of clarity about how long data should be retained—and who has the authority to make those decisions. Oftentimes, one person or entity cannot make a final decision; there are several stakeholders who need to be consulted or have a role in reaching the decision.

This section provides insight into two key questions:

1. Who are the stakeholders?
2. How are these stakeholders engaged to strategically and effectively manage information?

Although everyone in an organization has a responsibility to manage information, there are several key stakeholders who have a specific role in the overall governance of data, records, and information through their lifecycles, and they must work collectively and collaboratively to ensure consistency and compliance. Though the names and specific roles of the stakeholders vary depending on an organization's priorities, culture, risk appetite, regulatory obligations, and geographic reach, this guide provides general profiles of these stakeholders. The Information Governance Reference Model (IGRM) shown earlier represents the functional areas that are directly responsible for the governance of information across an enterprise in a unified framework.

WHO ARE THE KEY STAKEHOLDERS?

To help identify the key stakeholders, below are high-level descriptions of their typical responsibilities. Please note that titles of these stakeholders may be different in each organization and their responsibilities may be held by more than one role. For example, Legal/Privacy/Risk can all individually be responsible for determining the risk profile of an organization; conversely, Risk and Security could be merged into one single function.

(INFORMATION) SECURITY

The Information Security function is responsible for:

- Development, implementation, and management of the organization's security vision, strategy, policy, and programs
- Information security-related policy creation, technology selection and implementation, and monitoring and informing parties about malware, breaches, hacking, etc.
- Formally communicating policies and procedures to the business
- Enabling security standards dictated by customers, such as the government
- Informing the necessary parties when there are issues with breaches
- Issuing data classification codes (in conjunction with Legal)
- Remaining compliant with ISO and other regulatory bodies, as required

Depending on your organization, some of the responsibilities listed may be located in other functions, such as Legal or Information Technology. The lead of this function is typically the Chief Information Security Officer (CISO).

PRIVACY

The Privacy function is responsible for:

- Managing the risks and business impacts of privacy laws and policies
- Responding to regulator, shareholder, and consumer concerns over the use of personally identifiable information, including medical data and financial information
- Participating in the procurement process for vetting vendors and technologies
- Developing policies, privacy notices, and staying informed of international privacy law and its impact on data, records, and information management

In some organizations, the compliance component of this role is in the Risk or Compliance organization and the legal interpretation, advice, and counseling are in the Legal organization. The lead of this function is the Chief Privacy Officer (CPO).

RISK

The Risk function is responsible for:

- Protection of the organization's brand, finances, and operations by managing and mitigating risk exposures
- Understanding the organization's risk profile, including litigation, investigations, regulatory requirements, protection of private information, and protection of intellectual property
- Collaborating with Legal to create the "acceptable use" policy, and with IT to develop acceptable disaster recovery and business continuity processes
- Selection of, or removal of, SaaS/cloud providers
- Leading on-going education of employees regarding prevention of risk-related activities
- Providing input to key risk indicators and conducting periodic risk assessments

This function works closely with Records and Information Management (RIM), Legal, and IT to ensure the information risk is minimized. The lead of this function is typically the Chief Risk Officer (CRO).

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 retention requirements
- Providing guidance for the organization's records retention schedule, designation of date classifications, and policies governing email management, social media, mobile devices, and other electronic or networking devices
- Communicating any changes to the organization due to mergers, acquisitions, and divestitures
- Approving defensible disposition processes

This function communicates any changes to rules and regulations, including data privacy law with the RIM and IT teams, and collaborates with key Information Governance stakeholders. Two stakeholders that could be a part of the Legal function are Compliance and E-Discovery.

COMPLIANCE

The Compliance function is responsible for:

- Ensuring that the organization is aware of, understands, and meets the requirements of rules and regulations imposed by a variety of authorities (federal, state/provincial, and local governments; regulatory agencies; data privacy authorities; and industry groups)
- Determining internal metrics and controls
- Establishing an enterprise-wide monitoring and audit program
- Responding to and managing requests from regulators, auditors, investigators, customers, and other third parties

Compliance may also be a part of the Privacy or Risk functions.

E-DISCOVERY

The E-Discovery function is responsible for:

- Communicating and coordinating with business units and/or employees related to information that must be located, preserved, and produced to satisfy litigation and regulatory requirements
- Managing Freedom of Information Act requests
- Updating designated custodians (typically business owners and IT) on the status of the "holds" on information, including when information can be released for normal information lifecycle management
- Apprising RIM and IT teams when there are any changes to discovery requirements
- Instituting a repeatable process with associated guidelines to manage the spectrum of simple through complex litigation

E-Discovery may also report into the Information Technology function.

RECORDS AND INFORMATION MANAGEMENT

The Records and Information Management (RIM) function is responsible for:

- Drafting, publishing, maintaining, and monitoring compliance with the RIM Program policies and standards governing paper and electronic information lifecycle, including the records retention schedule
- Collaborating with key stakeholders (identified in this section) and the business to ensure alignment on and support of the RIM Program policies and standards
- Driving implementation support through training and on-going communications
- Identifying and gathering metrics to monitor compliance, determine remediation, cost containment through information lifecycle awareness and storage options, and destruction execution

- Participating with IT to integrate RIM requirements in existing applications and new software review, selection, and implementation
- Developing and leading a network of Business Liaisons to support business compliance and issue resolution
- Staying current with technology trends and the impact on information management (e.g. AI, Blockchain, cloud, big data, and BYOD)

This function may also be called Information Lifecycle Management (ILM). It collaborates with, and may sit in the Legal, Compliance, or Technology function.

BUSINESS

The Business (lines of business (LOBs), business units, and/or departments) function is responsible for:

- Ensuring compliance with Information Governance policies
- Managing information through its lifecycle by establishing the attributes, tags, indices, or metadata necessary for compliance as close to its creation as possible, e.g. flagging a piece of information as being confidential or containing personally identifiable information, or that it is an official business record belonging to a specific category of information
- Reviewing their data, records, and information for disposal according to approved defensible disposition processes and taking legal holds into account
- Collaborating with IT and RIM to determine how they can best take control of their information through technology and process
- Determining the "value" of the information they create, maintain, or receive beyond that of its "official" use; certain types of records may be used to determine marketing trends, track quality control issues over time, expand customer profiles and identify "bad actors" in a regulated environment

Once again, RIM should work with the businesses to help determine valuable information and how it should be managed in a secure and compliant manner.

INFORMATION TECHNOLOGY

The Information Technology (IT) function is fundamental to the success of Information and Data Governance. It usually comprises several specialty areas, including network security, workspace technology, systems architecture, and business application management. While traditionally this function was focused on technology and infrastructure, it's shifting to be more aligned with the business and its objectives. To that end, the Information and Data Governance goal of IT is:

- Increasing the ability to efficiently manage the high volume of data being created and received, and to eliminate costs, particularly around redundant technologies and storage
- Providing leadership for the proper protection and authentication of data and its availability for use, preservation, and disposition
- Collaborating with RIM, Risk, and Compliance to help with vendor management
- Determining appropriate disaster recovery and business continuity plans
- Managing identity and access management (e.g. access controls, onboarding/ offboarding, etc.)

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

DATA GOVERNANCE/MAINTENANCE

Data Governance assists business units and other functions in ensuring a consistent and controlled approach to the development and use of enterprise information assets and critical data elements across an organization. Data Governance is responsible for:

- Guiding the establishment of processes and systems sufficient to create, maintain, and share data in compliance with an organization's data standards and external regulations/laws
- Acting as the governing authority that implements a framework of controls that support effective and efficient management of data
- Assigning a Data Steward to the functions and businesses across the organization to conduct data governance/data management practice assessments through various tools such as the Data Maturity Model, Data Quality platform, and Data Standards implementation plans
- Focusing on data classification, protection, and quality, as well as getting the most value from data

Data Governance usually reports into Information Technology but could also be a stand-alone function.

Additional resources to broaden the understanding of this role are provided by the EDM Council. Described on its website as a "Global Association created to elevate the practice of Data Management as a business and operational priority," EDM's data standards and best practices can provide further insights into comprehensive information management.

HOW ARE THESE STAKEHOLDERS ENGAGED TO STRATEGICALLY AND EFFECTIVELY MANAGE INFORMATION?

Among the most critical values of these stakeholders is the ability to make prompt, reasoned decisions and avoid conflicts and bureaucracy, all within an accountability framework. The collaboration among these groups supports the development, buy-in, and promulgation of an Information Governance program that addresses the lifecycle of information. How are these stakeholders engaged? The best practice is to create a cross-functional Information Governance (IG) team of these stakeholders.

The IG team, led by a Chief Information Governance Officer (CIGO) or equivalent, and composed of cross-functional, senior-level key leads of the stakeholders will provide guidance and oversight to achieve unified governance across the various functions depicted on the IGRM. Since IG should extend across an organization's entire enterprise, there must also be proper geographic representation at the committee level that can speak to the concerns of the different jurisdictions in the organization. Collaboration among these strategic roles includes relying on common and specific functional content. Stakeholders should understand the value of data, records, and information, driven by expanded uses and requirements, and they should cope collaboratively with the costly and challenging growth in its volume, velocity, variety, and need for veracity.

This team would do the following:

1. Identify and classify content, recognize relationships and patterns, and thereby apply controls governing access, protection, retention, and disposition of content.
2. Execute governance strategies and operational plans, enabling risk reduction and cost effectiveness contributing to bottom line targets.
3. Identify and prioritize information risk and develop strategies to mitigate the risk.
4. Be an escalation point for resolution of potential conflict that may arise from the overlap in the dynamic matrix of stakeholder roles reflected in the IGRM.
5. Create, amend, and publish policy to support compliant practices across the enterprise.

Corporate requirements at the strategic level need not focus on carefully defining data and information apart from records; requirements for each should be viewed through a common lens given the coalescing interests such as analytics, security, confidentiality, and data minimization at the strategic level.

There is an opportunity to leverage common and related capabilities to strategically meet business, operations, and regulatory requirements. The IG team is the key to strategically and holistically governing the data, records, and technology functions of an organization.

OPPORTUNITIES TO SUSTAIN ALIGNMENT

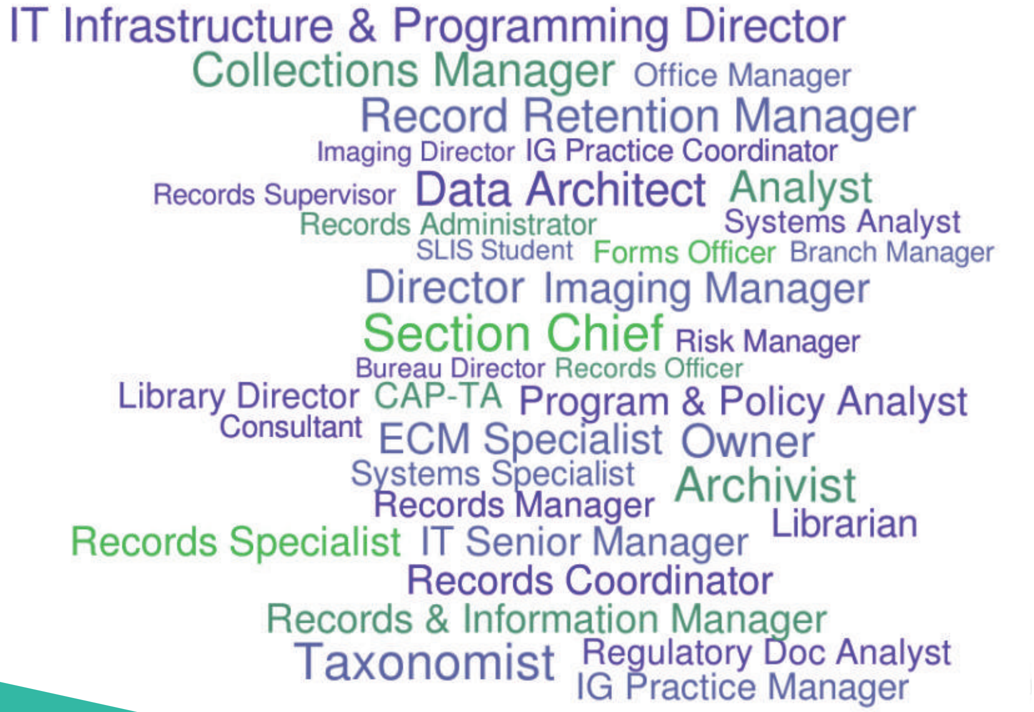
A number of tried and true approaches help build and maintain strategic relationships. These include the creation of governance boards and/or steering committees to make strategic decisions, generate buy-in to ideas, promulgate opportunities and requirements, and incorporate feedback from stakeholders with strategic importance. Producing regular reports on progress and showing success in addressing requirements and inefficiencies help to maintain effective governance structures.

ORGANIZATIONAL OBJECTIVES

The objectives regarding the management of data, records, and information vary depending on the priorities, culture, and other parameters of each organization. The goal is to form strategic relationships of the right mix of roles to effectively achieve short-term priorities and long-term goals. The LOBs and Chief Data Officer (CDO) prioritize business enablement and efficiency, but with a focus on protecting and controlling data, particularly the most sensitive data. Typically, Legal, Compliance, and Risk groups drive the initiatives that protect the organization. Technology has the unenviable task of satisfying the myriad and sometimes conflicting requirements across the enterprise. Operations and shared services enable the implementation of initiatives and execution of programs.

All content has an information lifecycle ending in disposition—either its elimination or historical preservation. To meet the short- and long-term objectives of an organization, all pertinent stakeholders must be concerned with the ownership, policies, requirements, procedures, identification, and classification of content. Knowing this, and executing governance strategies and operational plans, enables risk reduction and cost effectiveness, which contribute to bottom-line targets.

Lastly, the following graphic illustrates the complexity of commonly aligned roles and responsibilities that work together to address information-related business needs. Whatever the title, it's critical to ensure all relevant parties are included in the decisions made about managing data and records.



CONCLUSION

Even with all the compelling reasons we've covered in this guide, uncertainty as to how to address the intersection of IG and DG in a collaborative and strategic way remains. As interactions increase around the varied interests in both information and data management, the roles we identified must collaborate and learn, more or less, depending on their maturity and overarching organizational cultures.

While we likely will not persuade all of our partners and constituents to understand data, records, and information as we would like, being mindful of the perspective of our collaborators is critical to achieving our goals. A shared understanding, "seeing the field," can only help foster collaboration.

For now, continuing to learn and understand the goals and objectives of partnering functions and stakeholders is critical for effective digital transformation and the long-term benefit to our organizations. Priorities should include strong communication across an organization's leadership and the development of talent within each function, underpinned by vigilant collaboration. Only through cross-functional teaming can business goals and digital transformation objectives, along with on-going risk and cost-reduction efforts, be successfully met.

APPENDIX

USE CASE

This use case specifically demonstrates how one global financial institution has tackled the challenge of managing records, data, and information in a consistent, systematic way. Please note, some of its descriptions do not conform with those used previously in this guide.

BACKGROUND INFORMATION

An increasing topic of discussion related to records management is around the difference between data, information, and records. As more scrutiny is applied to data within a company, the lines between these concepts blur. Let's start with some definitions before illustrating the difference between these concepts.

DEFINITIONS

For fair comparison, most of the definitions below come from the International Organization for Standards (ISO) though Merriam-Webster provides a more common definition.

Data Element: A unit of data for which the definition, identification, representation, and permissible values are specified by means of a set of attributes (ISO/IEC 11179-3; 1994)

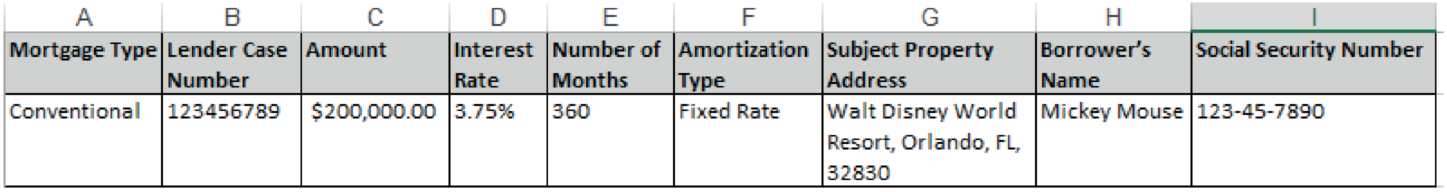
Data: An interpretable representation of information in a formalized manner suitable for communication, interpretation, or processing (ISO/IEC 2832-1; 1993)

Information: Knowledge that you get about someone or something: facts or details about a subject (Merriam-Webster)

Record: Information created, received, and maintained as evidence and as an asset by an organization or person, in pursuit of legal obligations or in the transaction of business (ISO 15489.1). NOTE: Retention requirements are applied to records based on laws, rules, and regulations.

For example:

An easy way to understand the difference between data, information, and records is to consider a common spreadsheet. Columns represent data, rows represent records, and the spreadsheet represents information. To make these differences more real, consider the illustration below. Consider this list containing one specific, real-life example in a mortgage business.



A	B	C	D	E	F	G	H	I
Mortgage Type	**Lender Case Number**	**Amount**	**Interest Rate**	**Number of Months**	**Amortization Type**	**Subject Property Address**	**Borrower's Name**	**Social Security Number**
Conventional	123456789	$200,000.00	3.75%	360	Fixed Rate	Walt Disney World Resort, Orlando, FL, 32830	Mickey Mouse	123-45-7890

Figure 1

Data: Each column represents data as there could be more than one mortgage on this list. For example, column D tells us the interest rates across all loans in this list. Column E tells us the number of months or loan term for all loans in this list.

Data Element: Each cell represents a data element where there is a specific definition, representation, or permissible use. In this example, the interest rate is 3.75%. The definition of this element could provide restrictions that interest rates have a minimum of 3% and a maximum of 4%. The chosen representation is using a % instead of decimals. Only numbers are permitted in this cell, no letters. NOTE: Retention requirements are not applied to data/data elements.

Record: The data elements across a row represent a mortgage loan which could be considered a record as it represents the transaction of business. A record represents the full transaction as knowing only the interest rate is irrelevant if the transaction has other required data to be valid (e.g., loan amount, number of months, etc.) NOTE: Retention requirements are applied to records.

Information: In this example, the spreadsheet contains a list of mortgage loans. This would be considered information to be used as part of the mortgage process.

A business perspective – Source documents and where data is acquired

There is a natural hierarchy in acquiring data, which begins with the source documents. Source documents can be records but in many cases are just the vehicle to collect the data that ultimately becomes a record. Your organization should make the determination of where a record is declared as such, whether it is the source document or data in an application.

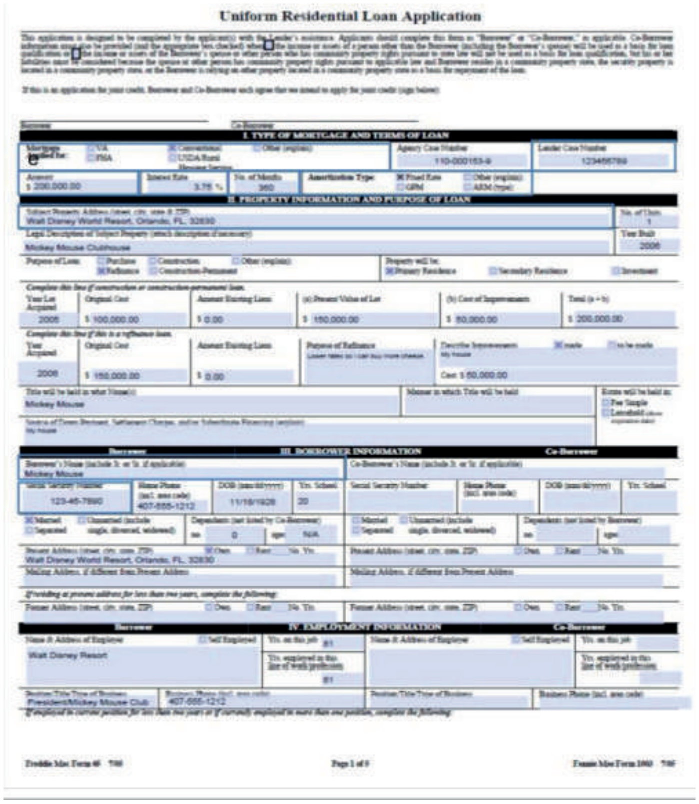
Source documents can be paper or digital, but the key is that all source documents contain data. Increasingly, source documents are born digitally, which makes acquiring data relatively easy when compared to paper. Paper documents must either be manually indexed by a human typing required data into an application or imaged/scanned with data extracted in a more automated fashion.

The example below represents a typical mortgage document. Highlighted are some of the fields containing data that can be captured in a system for further processing.

Data that can be collected from this document includes:

- Mortgage Type
- Lender Case Number
- Amount
- Interest Rate
- Number of Months
- Amortization Type
- Subject Property Address
- Borrower's Name
- Social Security Number

NOTE: Data shown in figure 1 above was acquired from the source document shown in figure 2, below.



Uniform Residential Loan Application

This application is designed to be completed by the applicant(s) with the Lender's assistance. Applicants should complete this form as "Borrower" or "Co-Borrower," as applicable. Co-Borrower information must also be provided (and the appropriate box checked) when □ the income or assets of a person other than the Borrower (including the Borrower's spouse) will be used as a basis for loan qualification or □ the income or assets of the Borrower's spouse or other person who has community property rights pursuant to state law will not be used as a basis for loan qualification, but his or her liabilities must be considered because the spouse or other person has community property rights pursuant to applicable law and Borrower resides in a community property state, the security property is located in a community property state, or the Borrower is relying on other property located in a community property state as a basis for repayment of the loan.

If this is an application for joint credit, Borrower and Co-Borrower each agree that we intend to apply for joint credit (sign below):

Borrower ____________ Co-Borrower ____________

I. TYPE OF MORTGAGE AND TERMS OF LOAN

Mortgage Applied for: □ VA □ FHA ☒ Conventional □ USDA/Rural Housing Service □ Other (explain):

Agency Case Number: 110-000153-9

Lender Case Number: 123456789

Amount: $ 200,000.00

Interest Rate: 3.75 %

No. of Months: 360

Amortization Type: ☒ Fixed Rate □ GPM □ Other (explain): □ ARM (type):

II. PROPERTY INFORMATION AND PURPOSE OF LOAN

Subject Property Address (street, city, state & ZIP): Walt Disney World Resort, Orlando, FL 32830

No. of Units: 1

Legal Description of Subject Property (attach description if necessary): Mickey Mouse Clubhouse

Year Built: 2006

Purpose of Loan: □ Purchase ☒ Refinance □ Construction □ Construction-Permanent □ Other (explain):

Property will be: ☒ Primary Residence □ Secondary Residence □ Investment

Complete this line if construction or construction-permanent loan.

Year Lot Acquired	Original Cost	Amount Existing Liens	(a) Present Value of Lot	(b) Cost of Improvements	Total (a + b)
2005	$ 100,000.00	$ 0.00	$ 150,000.00	$ 50,000.00	$ 200,000.00

Complete this line if this is a refinance loan.

Year Acquired	Original Cost	Amount Existing Liens	Purpose of Refinance	Describe Improvements ☒ made □ to be made
2006	$ 150,000.00	$ 0.00	Lower rates so I can buy more cheese	My house Cost: $ 50,000.00

Title will be held in what Name(s): Mickey Mouse

Manner in which Title will be held:

Estate will be held in: □ Fee Simple □ Leasehold (show expiration date)

Source of Down Payment, Settlement Charges, and/or Subordinate Financing (explain): My house

III. BORROWER INFORMATION

Borrower				Co-Borrower			
Borrower's Name (include Jr. or Sr. if applicable): Mickey Mouse				Co-Borrower's Name (include Jr. or Sr. if applicable):			
Social Security Number	Home Phone (incl. area code)	DOB (mm/dd/yyyy)	Yrs. School	Social Security Number	Home Phone (incl. area code)	DOB (mm/dd/yyyy)	Yrs. School
123-45-7890	407-555-1212	11/18/1928	20				

☒ Married □ Unmarried (include single, divorced, widowed) □ Separated — Dependents (not listed by Co-Borrower) no. 0 ages N/A

□ Married □ Unmarried (include single, divorced, widowed) □ Separated — Dependents (not listed by Borrower) no. ages

Present Address (street, city, state, ZIP) ☒ Own □ Rent ___ No. Yrs.: Walt Disney World Resort, Orlando, FL 32830

Present Address (street, city, state, ZIP) □ Own □ Rent ___ No. Yrs.:

Mailing Address, if different from Present Address:

Mailing Address, if different from Present Address:

If residing at present address for less than two years, complete the following:

Former Address (street, city, state, ZIP) □ Own □ Rent ___ No. Yrs.

Former Address (street, city, state, ZIP) □ Own □ Rent ___ No. Yrs.

IV. EMPLOYMENT INFORMATION

Borrower			Co-Borrower		
Name & Address of Employer: Walt Disney Resort	□ Self Employed	Yrs. on this job: 81 Yrs. employed in this line of work/profession: 81	Name & Address of Employer:	□ Self Employed	Yrs. on this job: Yrs. employed in this line of work/profession:
Position/Title/Type of Business: President/Mickey Mouse Club	Business Phone (incl. area code): 407-555-1212		Position/Title/Type of Business:	Business Phone (incl. area code):	

If employed in current position for less than two years or if currently employed in more than one position, complete the following:

Freddie Mac Form 65 7/05 Page 1 of 9 Fannie Mae Form 1003 7/05

Figure 2

Now that data has been acquired from the source document, your organization needs to make some decisions:

1. Is the paper source document considered the record?
2. If the source document was imaged, is the image the record?
3. Is the data collected from the source document and processed in an application the record?
4. Can the original paper document be destroyed?

Depending on decisions made, you need to either store or destroy the original as the data in an application could potentially be the record for your company.

Organizing records to support data architecture

Let's assume the data acquired from the example loan in figure 2 is considered the record. How do you organize and protect the integrity of that record while making the data available for downstream usage?

Figure 3 below shows a simple database architecture that maintains the loan data.

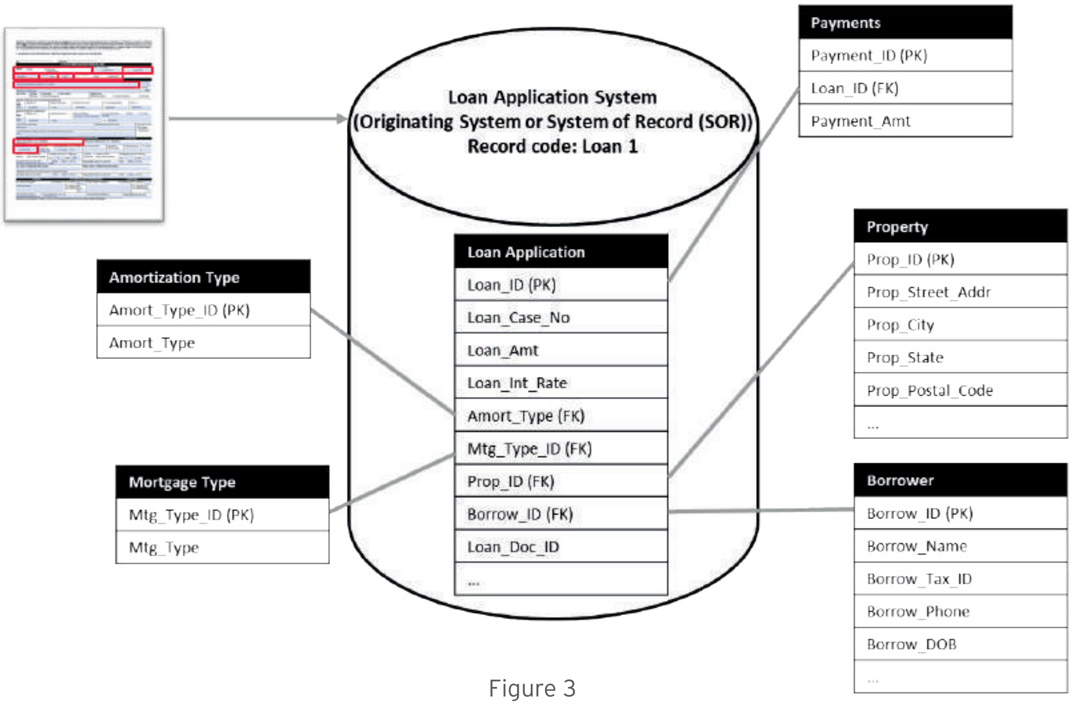


Figure 3

The loan application table contains all the data acquired from the original source document and is stored with all the controls to protect the integrity of the record. Retention requirements are applied to the record ensuring that it is neither over nor under retained. Authorized disposition may be met by having a separate data source that captures when loans are paid in full or otherwise terminated; the data of that trigger event is captured, and retention policy is associated with that source that then initiates disposition in the application when satisfied.

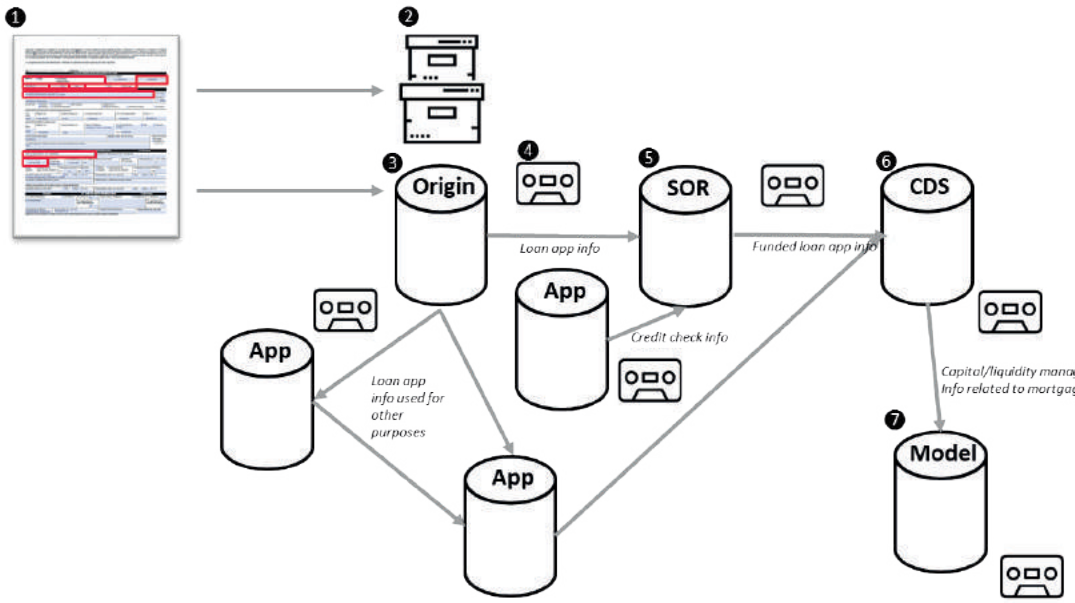
To simplify and optimize storage and usage, the data can be organized using database design principles to normalize the data like the tables referenced by the loan application table.

Since the record is stored in this manner, all or a portion of the data from the record, can then be used for downstream purposes if needed and appropriate. A few examples of downstream usage of the example loan record and related data include:

- Operational or regulatory reporting
- Relationship management
- Credit scoring
- Liquidity calculations
- Modeling and analytics

NOTE: While the data can be used downstream for these purposes the original record is retained and protected.

Figure 4 below demonstrates the complexity that can come from using data contained in a record for downstream purposes. The data doesn't stop at one "hop" downstream. It can continue to be processed in different ways, creating more records for different purposes.


1
2
3
Origin
4
5
SOR
6
CDS
Loan app info
Funded loan app info
App
Credit check info
App
Loan app info used for other purposes
App
Capital/liquidity management Info related to mortgages
7
Model

Step	Location	Record Code / Description
1	Source Doc	LOAN 1 – Mortgage application
2	Off site storage	LOAN 1 – Paper version of mortgage application stored offsite
3	Origin	LOAN 1 – Data lifted from mortgage application and stored in SOO
4	Backup	BACKUP 1 – Backup of data stored in database for DR purposes
5	SOR	RELATIONSHIP 1 or another record code – data combined to reflect customer account record
6	CDS	REPORTING 1 / LIQUIDITY 1 – data combined with other input to create new records for capital management. Copies of data also present.
7	Model	MODEL 1 - data extracted from ADS for modeling purposes and stored for multiple economic cycles.

Figure 4

Once data from a record is made available, it can continue to be used for many different purposes, if not controlled. Your company will have to determine where data from records is considered a copy or a net-new record. This requires partnership with your Legal and Compliance teams who can work to ensure that you only retain the minimum amount of data, and by extension records, if needed according to laws, rules, and regulations.

800.899.IRON | IRONMOUNTAIN.COM