# The Complete Compliance and Ethics Manual 2023
# Creating an Effective Data and Information Governance Program

By Virginia MacSuibhne and Leslie Stevens[2]

## Introduction

There are many important reasons why organizations have created and are currently reinvirgorating their data and information governance programs, a subject formerly known as records and information management. First, records and information document critical business activity and access to them is necessary for both effective business operations and data-led business imperatives. Second, information and data sources continue to increase exponentially and, therefore, the need to properly manage and protect them as critical assets from increasing cyberthreats is greater than ever before. Third, records and information are often required by government agencies for licenses and other government filings. Fourth, records are necessary for the prosecution or defense of litigation or legal claims. Fifth, the storage of excess data and information can be costly, especially with the rise of randsomware and other cyberattacks. Sixth, records and information can be a major source of clues about potential ethics and compliance and privacy issues and violations. Seventh, with the proliferation of data protection and privacy laws, regulations demand that organizations are accountable to ensure personal information is only retained where necessary for legiteimate business purposes and in accordance with varying legal frameworks.

A well-defined and well-executed data and information governance program can capture and categorize the types of data and information an organization has in a meaningful data map. It can ensure that the data and information necessary to run the business remain available, that the data and information needed for government authorities and litigation are accessible, and only necessary data and information are retained in an efficient and accessible manner for the required periods. In addition, a well-defined data and information governance program can provide invaluable support for the ethics and compliance, privacy and information security functions with critical information about the types of data that are regularly created in the business, how the data flows, and whether there are any unusual activities that might cause concerns or require further investigation.

### Key Reasons for a Data and Information Governance Program

Data and information governance programs allow companies to:

- Manage data/information explosion and simplify and control access to data
- Document business activities for business continuity
- Comply with government requirements, including data protection and privacy laws
- Prosecute/defend litigation or claims
- Manage storage costs
- Identify key information assets and protect them

- Support ethics & compliance, privacy and information security functions
- Respond efficiently to information security incidents

An effective data and information governance program can therefore be a key component of any workplace ethics & compliance, and privacy and information security program. Core components of an effective data and information governance program should include, at a minimum:

- An understanding of the tools, platforms, and applications that the business uses to generate, store, retain, and protect information;
- A clear and easy-to-use records retention policy, schedule, and procedures;
- A simple and easy-to-use data classification or sensitive information labeling policy and procedure;
- A well-thought-out and documented claim, audit and litigation hold process;
- A governance structure with senior leadership buy-in and meaningful representation from the business; and
- Clear and actionable educational materials and training on the data and information governance program.

Each will be discussed in greater detail below.

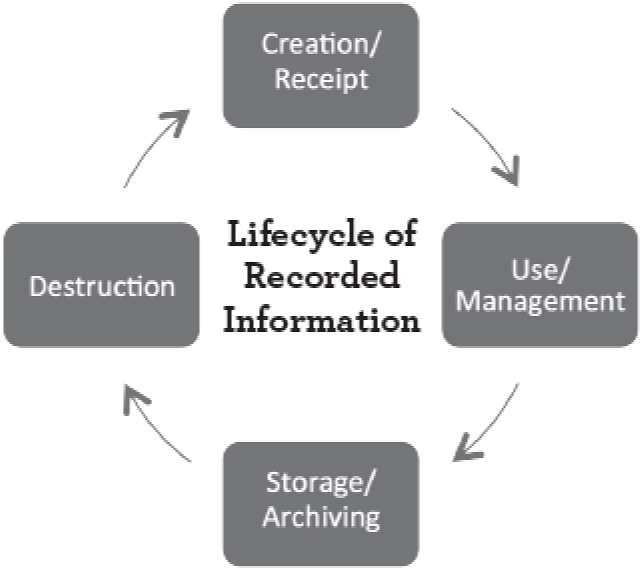
## Data and Information Governance

To begin building a program, the first consideration on which a business should focus is what the business is, does, and/or makes and sells. Next, an organization should identify the types of data and information the organization generates (e.g. personnel files, contracts, purchase orders, marketing collateral, client records, product development files, etc.). Next, the organization should determine the forms and formats its data, records, and information take (e.g. paper, electronic, and other form such as prototypes, models, discs, microfilm). At this stage, if the organization does not already have a documented data classification or sensitive information labeling policy and procedure, the organization should determine what of this information is considered the most sensitive and confidential, outlining the procedures that must be followed for such information types.

### Initial Considerations for Launching a Program

- What is the business of the organization?
- What types of data and information does the organization generate or process?
- What types of data and information are subject to special protections and procedures due to sensitivity/confidentiality?
- What form and format does the data and information of the organization take?

## The Life Cycle of Recorded Information



Primarily, an organization must identify the scope of the data and information governance program. A program needs to address the entire life cycle of all recorded information generated by, at, or on behalf of the organization from the moment of creation or receipt through use and management, storage/archiving, and destruction. A program should address both official business records and information, as well as that data and information that are personal or for convenience of the organization's workers.

## Creating an Effective Data and Information Governance Program Infrastructure

The goals of any data and information governance program should be to: 1) ensure all key business data is identified and has an appropriate life cycle, 2) ensure that all workers know when they are acting as custodians for data and know how they are expected to manage that data, including where to store it, who and how to grant access to the data, and when and how to delete it, and 3) ensure that as data and information types and forms change, the program evolves and is appropriately updated. To accomplish these goals, there are several components for consideration, including:

- An effective team working collaboratively in departments, groups, and functions, such as IT, privacy, and legal;
- A clear and appropriate policy or set of policies;
- A clear and well-defined retention schedule;
- A simple and easy-to-follow data classifcation or sensitive information labeling policy and procedures;
- A data map of key data in the organization and how it flows to, from, and through the organization (this is particularly recommended for data sets that include sensitive or personally identifiable information);
- Custodian identification;
- Effective tools and systems and processes to monitor and manage changes in processes, tools, or other relevant matters;
- Effective training and awareness for all workers at the right level about the program; and

- A well-defined process for issuing and managing records holds (and discovery for litigation).

Each will be discussed in turn.

**Data and Information Governance Program Components**

- Data and information governance team
- Data retention policy
- Data retention schedule
- Data custodian identification
- Tools and systems
- Education and training
- Hold management process for audits, investigations, and litigation

## Data and Information Governance Team

A key to the success of any program is the team. It is important to ensure that there are sufficient resources dedicated to the data and information governance program for the size and complexity of the organization. One size will not fit all. An organization of 1,000 employees located across three sites in the United States with six business areas will have different resource needs than an organization with 20,000 employees located across 10 sites in four countries and three business areas. Likewise, a business that deals in generating and selling data will have different needs than a business that makes and sells food products. At a minimum, it is recommended that every organization have a lead person who is responsible (whether full-time or otherwise) for data and information governance. Equally, it is critical that this person is supported by individuals in the business who know and understand the business and how data in those individual functions are generated and used throughout the information lifecycle.

The following records and information management roles and responsibilities may be necessary:

- **Assessment of current state of data and information governance**

  This should include the nature of business, types of data and information, forms of data and information, and current practices for data storage, retention, and destruction. This assessment will require interaction with every business group and a close working relationship with information technology experts and, in many cases, with the legal department and privacy subject matter experts.

- **Data policy and retention schedule development**

  This task can be assigned to a project team, committee, or single person (consultant or employee) as appropriate. Development of the appropriate retention periods may require consultation with in-house or outside legal counsel regarding local, state, federal, and country regulations.

- **Business Area data coordinators/subject matter experts**

  These people can liaise with the program office or personnel and assist with ensuring personnel in their specific business area understand the applicable portions of the data retention policy, follow the policy and retention schedule, and see that all new developments are fed back for program updates.

- **Hold management and coordination**

  Audits, investigations, and litigation (actual and potential) bring a host of specific retention requirements that may conflict with the general data and information management process. It is therefore important to have personnel in the program office, legal department, and IT groups who understand these issues and are prepared to mitigate the risks with appropriate issuance of data hold notices, systems holds, and review and collection of information potentially relevant to litigation.

## Data and Information Management Policy

Development of the data and information management policy and a retention schedule is at the heart of most programs. The policy is where an organization should clearly articulate expectations about to the creation, management, storage, and destruction of data and information. Minimally, a policy should:

- Identify and distinguish business records from convenience records and personal from business records;
- Provide compliance expectations and the potential consequences for failure to comply;
- Identify where employees can find the appropriate retention periods;
- Direct employees on how to manage data and information;
- Direct employees on how to manage physical records on-site or any other physical artifacts, such as prototypes or other items;
- Direct employees on how to store records and information on- and offsite, including direction on appropriate storage and destruction of records for remote workers;
- Provide details on any process or documentation required prior to destruction of official business records;
- Provide guidance on any process required when terminating supplier relationships to ensure supplier or other third party of the destruction or return of official business records and other business information;
- Educate employees about the potential for litigation or other holds and the process for managing those holds; and
- Notify people where they can seek guidance or additional information.

Refer to the sample policy in the appendices at the end of this article.

## Data Retention Schedule

In addition to the policy, or as a component of it, organizations should also create and adopt a data retention schedule identifying the length of time each category of information should be retained. Retention requirements are a mix of legal, regulatory, business and best practices rules applied to various categories of records and information. There are some clear legal/regulatory mandates for how long certain types of records/ information must be kept (e.g. The Occupational Safety and Health Administration, OSHA, requires copies of records and information related to employee hospitalizations related to work-related injuries or illnesses be maintained for 30 years). The statute of limitations for certain types of legal claims can also drive some retention dates (i.e. contract claims generally have no more than a three-year statute of limitations, so records related to contracts are often kept three or more years from the termination date to ensure availability in the event of a dispute that arises during the statute of limitations). Further, contractual agreements of an organization generally have a term and/or termination date and some continuing obligations which may drive retention periods. The business area(s) may also have their own vision and desires for retention periods based on the way the business runs. Regardless of the driver of the retention period(s), it is important to supplement the data management policy with a data retention schedule. This schedule should advise how long different types of data and information must be retained, when such data must be deleted (particularly for compliance with data protection and privacy laws) and the trigger date for the running of the retention period and provide concrete examples of records that fall into each record class. A sample retention schedule excerpt is included in the appendices at the end of this article.

In creating the data retention schedule, organizations must consider how many different retention codes and periods they want to create and enforce. Some businesses may opt to retain all records for only the minimum period required for legal, regulatory, or business reasons, which may result in hundreds of different retention categories and periods. Other businesses may opt to adopt fewer retention categories with retention periods that might be longer than specifically required, in favor of simplicity of the program. A further trend to consider is the move to retention schedules setting a maximum retention period due to the requirements of data protection and privacy laws, which require personal information to only be kept for the minimum amount of time necessary to fulfill legitimate business purposes. Such considerations are important decisions for each organization to make based on the risk profile of their records and their risk appetite.

## Identifying Data Custodians

Another critical component in a data and information governance program is identifying data custodians. These people are responsible for maintaining the single official business copy or information and for providing those responsible for data and information governance programs with practical guidance and updates on how the business is generating data. This is critical to inform timely changes to policies, procedures, education, and training for each organization. For example, an HR manager may be tasked as the company custodian for all official company personnel files, while an IT manager may be tasked as custodian for all electronic systems, servers, and back-ups. Effective data custodianship entails each custodian advising the program with updates on new types of information and data being generated in their function and acting as the first point-of-contact for that part of the business when it comes to questions regarding the program. Given the electronic tools and mobile devices in abundance today, as well as copiers, scanners, email, and other technology, there are inevitably multiple copies of any single piece of information. Identifying and publicizing single data custodians can therefore help create efficiencies and reduce costs and ensure that duplicates are retained only as convenience records so long as needed, but do not become part of the business records and information archive. In addition to official custodians, litigation will also involve specific witness custodians who may have relevant information (official business or convenience records) by virtue of their role in the company or interactions on a specific matter.