COSMOS
Navigate the Compliance Universe

CEP Magazine - November 2023

**Mark Diamond** (markdiamond@contoural.com) is CEO of Contoural Inc. in Los Altos, California, USA.

# Who should own records management? Part 1

By Mark Diamond

Compliance and data risks are hitting companies from all sides. New and expanded legal and regulatory recordkeeping regulations require more records to be retained and, in many cases, for longer periods. New and emerging privacy rules require that personal information needs to be protected and deleted when there is no longer a legitimate business need. Increasing overretention of paper—especially electronic information—places companies at risk during e-discovery. This occurrs in an environment where many employees spend the majority of their time working from home and seemingly want to save all their email, files, and other electronic information forever. This overretention increases data storage burdens and increases compliance risks. Worse, many companies have so much electronic information everywhere that they are not only noncompliant but so disorganized that employees can't find information they need in the clutter.

Traditionally, document retention and disposition are handled by a records management function. Yet, these newer challenges are not limited to records retention and disposition. In response, many companies are launching comprehensive information governance programs. These initiatives combine previously siloed records management, e-discovery, privacy, and other data security programs into a coordinated program with single workstreams that address multiple compliance regimes.

While clearly compliance should be involved as organizations upgrade records management functions in information governance, the question is raised: Who should own it? And by the way, who pays?

## Older management approaches are not working

Most companies have traditional, siloed records management practices, somewhat disparate from privacy, information security, and technology programs. Yet, in today's environment, this traditional approach falls short in three distinct ways. First, many traditional records programs rely heavily on manual employee processes. They are built on paper-based processes and depend, to a large degree, on employees to manually classify, tag, or move records into certain storage areas. These types of processes worked fairly well for paper. But today, more than 95% of the information a company receives is electronic. Even most paper documents are copies of electronic information. Paper-centric processes work poorly with electronic information. This is often the source of huge compliance gaps in records retention programs.

Next, standalone records programs can—and increasingly do—conflict with other compliance requirements. For example:

- Records management programs' retention requirements can conflict with privacy rules requirements for limiting the retention of personal information.

- Records retention processes that require ongoing deletion can undermine information that should be preserved under legal holds.
- Intellectual property management may be undermined by e-discovery data cleanup projects that inadvertently delete files and emails documenting the organic development of intellectual property.
- Data deletion initiatives can sometimes delete valuable business information employees need to do their jobs.

Finally, many programs ignore the most serious effect of electronic information overload: employee productivity. The average employee sends and receives more than 165 emails per day and creates or handles more than 20 files. Believing that they may need this information at some point in the future, many employees adopt a "save everything forever" approach. Employees who believe they need to save everything get caught in a trap of their own design (or lack of) and discover it is difficult to find valuable or relevant information within the clutter. Our surveys have shown that employees waste, on average, three hours per week—typically five minutes at a time—looking for useful information within their vast stores of redundant, obsolete, and transitory files. Poor information management ends up being a significant drain on employee productivity.

## Developing information governance programs

Increasingly, organizations are taking a unified information governance approach to controlling their documents and data. Instead of having multiple different initiatives at a departmental or divisional level, an organization-wide information governance program strives to create work streams that address common needs and, at the same time, minimize risk. It seeks coordinated control of data and documents for retention, business use, access, and disposition. Information governance recognizes that the key is gaining effective control of data and documents foremost and that good control through a single program can serve multiple records, discovery, privacy, and productivity matters.

A fundamental element of most information governance initiatives is combining legal and regulatory requirements with employee behaviors and business needs—with a very strong focus on measurable execution. No two information governance programs will necessarily look the same from organization to organization, as they must reflect the differing business realities that organizations face.

Information governance programs need to be both comprehensive in their approach and tactical in their execution. Taking a big-picture view can allow single initiatives to accomplish a number of business goals. Successful programs are developed with this larger view in mind. At the same time, it is important that these initiatives be broken into discrete tasks and that the benefits can be both measured and easily understood. While formal definitions may be technically accurate, often, it is more useful to describe these programs in plain, simple terms.

What's more, multiple groups may undertake similar tasks—such as data mapping—independently. Also, the needs of employees and business units are often ignored. It is common to find disjointed initiatives and a lack of coordination among groups, which are both ineffective and wasteful.

## Who should own information governance?

Everyone wants better control of information and data because doing so provides cost savings, productivity, innovation, and compliance benefits; however, often, no one group wants to end up owning the whole problem. The result is that many will see the need, but no one speaks up to say these challenges need to be addressed. Organizations get stuck, and the problems just get worse.

Responsibility for managing documents and data may fall across legal, records management, compliance, privacy, IT, information security, audit, human resources, and individual business units. Traditional programs, however—where responsibility is siloed—fall short. It is a problem many groups share, and yet no one group really owns.

- **Records management**: May be responsible for official records but not management and control of the nonrecord documents.
- **Compliance**: May be responsible for policy creation but depends on other groups to execute these policies.
- **Privacy**: Worries about privacy data in both records and nonrecords but is limited in its ability to drive disposition.
- **IT**: Manages data storage but not the actual content (which is owned by the business units).
- **Litigation**: Is often focused on matter-specific litigation but with no charge to proactively address management of documents and data outside of litigation.
- **Information security**: Is responsible for securing the firewall but has little say on what privacy data is stored where.
- **Business units**: Often do not care about any of this and want to be left alone to run the business, except they cannot even find their own important information in the clutter.

## The difference between information governance and data governance

What's the difference between information governance and data governance, or are they the same thing? How should each be managed? This area of significant confusion often comes up when an organization is considering launching an information governance initiative. Information governance and data governance are different yet complementary activities. Understanding the differences and intersections is key to keeping both on track.

Information governance addresses records and information management, litigation readiness, control of private and other sensitive information, and employee productivity. Information governance primarily addresses paper, semistructured media such as email, and unstructured media, including files and sometimes databases in structured applications. Data governance is defined as the processes and policies designed to ensure data is managed as a single point reference. It is about leveraging large amounts of data to answer big questions, such as who to sell to, how to price products, and what new markets should be approached. It encompasses areas such as master data management, data quality, and data modeling; it often uses newer types of technology, such as Hadoop, that can pull together different data sources. Data governance has long been associated with structured data living in a type of database (called "relational") but can also incorporate individual files or even emails. These types of projects are sometimes called "big data" projects and serve to drive revenue or increase profits.

While both initiatives strive to manage data better, the tasks, outputs, and skills required for each are different. Without a clear understanding of how these areas are different, it is easy for information governance activities, such as creating more efficient discovery processes, to get lost in a larger data governance agenda. Note that a strong information governance program can complement and assist a data governance initiative. For example, ensuring that emails and files ingested into a data governance "data lake" do not contain privacy or other sensitive information can keep the data lake "unpolluted" and compliant. When contrasting these programs, focus on project tasks and outputs and avoid esoteric technical definitions, which will help clear up potential confusion.

## Information governance ownership structures

Traditional records programs historically have reported to compliance or legal groups, but does the same hold true for larger information governance programs? We see three types of program ownership.

### Single-department ownership

| Pros | Cons |
|---|---|
| Easier to get started | Very difficult to fully execute |
| Centralized ownership/control is easier to manage | IT is often too focused on electronic records |
| Good when other departments offer only weak support | Often ignores or shortchanges needs of other constituencies |
| May work well in small to medium organizations | Hard to scale to large or global organizations |

**Table 1: Pros and cons of single department ownership**

Sometimes, a single department—such as legal or IT—has ownership of most parts of an information governance program (see Table 1). This structure is often a legacy of when records management reported to legal and was primarily responsible for managing paper. That structure is now changing. For example, records management responsibilities are expanding to include electronic documents and privacy, yet the group continues to report directly to the same function (usually legal).

The advantage of single-department ownership is that roles and funding are clear. Furthermore, the institutional knowledge of past practices is retained within the same group. For example, the facilities group, having always managed paper, knows where the paper repositories live. The clear disadvantage of this approach is that both the skills and capabilities for executing these programs lie across multiple groups. The facilities group is not likely to be an expert in the archival of electronic information and, therefore, is likely to promote the continued printing and retention of hard-copy documents.

This model is becoming less common. As organizations understand the requirements of these initiatives, ownership is often transitioned to multiple stakeholders. Organizations wanting to embrace this model type need to ask themselves if it will really work for them.

### Chief information governance officer responsible for multiple functions

| Pros | Cons |
|---|---|

| | |
|---|---|
| C-suite level legitimization of information governance function | Finding the right person can be challenging |
| Budget control independent of legal, IT, and other departments | Must successfully navigate entrenched owners of information governance program elements |
| Centralized control of all information governance functions | Multidiscipline expertise required |

**Table 2: Pros and cons of officer ownership**

During the past few years, there has been much discussion about the creation of a chief information governance officer (CIGO) position who has direct responsibility for many (if not most) components of an information governance program (see Table 2). While the CIGO ownership model implies a type of economy of scale, we have found that many departments are unwilling to cede control, ownership, and budget to another. Today, this position remains relatively rare.

## Cross-functional steering committee ownership

| Pros | Cons |
|---|---|
| Organizational buy-in and consensus | Requires strong participation from each constituency |
| Covers all information governance functions without centralizing control | Steering committee may not be seen as powerful as CIGO/central authority |
| Easier to locate and assign resources | |
| Group of stakeholders may hold more sway than single department or individual | |

**Table 3: Pros and cons of committee ownership**

By far, the most common approach when launching an information governance initiative is creating a cross-functional committee composed of multiple stakeholders (see Table 3). Typical committee members include compliance, legal, IT, privacy, audit, risk, and sometimes human resources and business units. Each stakeholder

remains responsible for its area of expertise (legal still creates policies, for example), but these activities are done through an integrated and coordinated plan. Most companies with successful information governance programs take this type of cross-functional approach.

Rethinking and reorganizing records management, data retention, privacy, and e-discovery into a cross-functional approach reduces the overall workload, decreases conflicts, and helps "stuck" programs get unstuck. The next article in this series will address how to start an information governance steering committee.

## Takeaways

- Organizations face new requirements and risks from over-retention of documents and data.
- Traditional siloed records programs are not effective at addressing these risks.
- Organizations are upgrading their records programs into more comprehensive information governance programs.
- Information governance is different but complementary to data governance.
- There are three types of program ownership structures; a steering committee is the most common and successful ownership model.