COSMOS
Navigate the Compliance Universe

CEP Magazine - December 2023

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

Who should own records management? Part 2

By Mark Diamond

This article is the second in a two-part series. Part 1 explored how siloed records management and information governance programs are difficult to execute and how most organizations are managing these efforts through a cross-functional steering committee.[1] Once the question of who should be involved is addressed, the next issue naturally arises: Who should pay for these programs? Part 2 explores which groups typically fund records and information management programs, which typically are involved, and strategies for launching or relaunching these efforts.

The elephant in the room: Who should pay?

While many groups within an organization see benefit in developing a strong information governance program, this enthusiasm is muted by one overriding concern: Which department is going to pay for this type of program? IT thinks compliance should pay because compliance will benefit from better risk management. Compliance thinks IT should pay because technology is involved. Or is it the business units who should pay? One of the risks in engaging a number of stakeholders in this discussion (and understanding their needs) is that it also creates conflicting expectations about who should pay. There have been situations where an email archiving system, for example, would have saved a company literally millions of dollars; however, the project was stalled due to arguments over who would pay. The greatest risk is that no one initiates this discussion for fear that speaking up first will somehow tag them as project funders.

Experience has shown that getting these issues out on the table early it is best. Clearly, information governance initiatives do cost money, but they can save even more money. Often, when the committee highlights the risks of not having a program, senior management will fund or start funding these programs through other sources. Some organizations have been successful in attaching these initiatives to risks that have been highlighted by the board of directors' audit committee. Sometimes, these committees have negotiated that legal will pay for the policy and IT will pay for the technology components.

Why compliance should be involved

When faced with information governance challenges, often the first question asked by compliance is: Why me? Compliance asks if and when they should be involved and wonders if it is better to let this be entirely an IT initiative—especially as a big focus is on the remediation and proper management of electronic data. At a time when many compliance department budgets are being scrutinized, it is fair to ask if they need to be the ones to lead this dance. In a word, yes. Compliance should participate in information governance programs for the following reasons:

- **Compliance experiences the pain of poor information management**: Not knowing where information resides forces organizations to drive up risks and costs directly. Failure to retain and provide accessible records can make dealing with regulators more difficult. Privacy and other sensitive information stored in the wrong place can greatly increase the likelihood of a data breach. Compliance, perhaps more than any other group, bears the consequences.
- **Compliance owns many policy components**: In most organizations, records retention and destruction, privacy, legal hold, and other key information management policies are legal's purview. It is critical that these policies be designed to be both compliant and executable. These policies should be created or updated early in the process.
- **Compliance helps avoid risk**: Part of compliance's charter is to proactively identify and avoid organizational risks. Perhaps more than any other group, they must be forward-thinking, anticipating changes in the legal, regulatory, and business environment and preparing the company to deal with these changes.
- **Compliance often has a respected voice in senior management**: Unlike other groups, compliance exerts a tremendous influence within an organization. Its voice is respected by both senior management and boards.
- **Information governance creates an opportunity for compliance to add additional value**: Organizations often start executing information governance programs to address legal or compliance issues and find that these programs also drive employee productivity and save money. These programs often change from something an organization needs to do to something it wants to do. In-house legal departments can demonstrate value by spearheading these programs.

Developing an information governance steering committee

An effective information governance initiative can be a big win for an organization, and getting started can be tricky, as many of these types of initiatives veer off the road and get stuck in the mud. How it is approached and with whom—decisions made early in the process—often dictate the success or failure of a program. While every organization is different, successful programs share some common approaches.

One of the biggest challenges in starting an information governance program is getting separate functions with separate budgets to work together on an integrated initiative. To overcome these challenges, in-house counsel—working with IT and others—should consider forming an information governance steering committee.

Steering committee members can include:

- **Compliance**: Privacy, audit, risk management
- **Legal**: Records management, litigation
- **IT**: Messaging, infrastructure, information security
- **Business units**: Human resources (HR), engineering, finance, etc., with the final composition varying from organization to organization

While the temptation may be to develop the strategy alone (or with a small group) and then engage other groups later in the process, starting with a larger group is better. Although a larger group may seem unwieldy, it is better to be more inclusive earlier in the process than having an excluded group stall the initiative later on.

Early on, roundtable discussions should be conducted to identify issues and generate stakeholder buy-in. A suitable senior management sponsor (or sponsors) to whom the committee is accountable should also be identified. A charter outlining the specific business issues to be faced, responsibilities of team members, and expected business benefits of the information governance program should be developed.

Teaching others about the benefits of records management can seem impractical, but there are approaches that work. Rather than trying to communicate the entirety of information governance, focus on the benefits it provides to each stakeholder. Consider stakeholder and other employee pain points and the risks inherent in their daily work, and propose individual benefits provided by better records management.

Information governance committee authority

An effective information governance committee strikes a balance of including committee members to decide on significant and cross-functional issues while allowing individual business units the latitude to execute their projects or pieces.

Some areas of committee authority include:

- **Policy decisions**: Committees often review important policy decisions, including retention, data security classification, employee use of portable devices, such as cell phones (known as "bring your own device" or BYOD policies), and other vital areas affecting what and how information is managed.
- **Roadmap**: The committee should be active in the development and review of the overall information governance roadmap, including prioritization of projects, time frames, and ensuring that these roadmaps do not conflict with other existing corporate initiatives.
- **Process approval**: Committees should review and approve retention, disposition, discovery, and other information governance processes.
- **Technology review**: Committees often provide input and review of major technology selections, including enterprise content management and archiving systems. While traditionally these decisions are the exclusive domain of IT, savvy IT organizations will realize that allowing this type of input will greatly increase adoption of these technologies when it is time to implement them.
- **Training**: It's essential to account for both group coordinator and individual training plans.
- **Internal communications**: Responsibility should include messaging and communication strategies to business units and employees.
- **Organizational development**: Once a program is developed, they oversee how it will be sustained and who will be responsible for which parts.
- **Milestone achievement**: Like all successful projects, they should identify and report on major milestones against the project calendar.

Sample agenda for first meeting

In-house counsel driving the creation of an information governance committee should carefully plan their first agenda. Lack of an effective information governance program clearly causes pain—especially for the legal group—and often, the best strategy for in-house counsel during these meetings is to let others discuss and realize how these issues affect their own departments. This is an opportunity to build buy-in from other groups. Some critical questions to be addressed during the first meeting are:

- What pain is being experienced due to too much and unmanaged information?
- Who else should be involved in addressing these pains?
- What should the committee charter be?
- How does the committee create a "plan for a plan" to address these issues?
- What is the committee's timetable?

Getting IT, business units, and other stakeholders on board

The first and perhaps hardest part of launching an information governance initiative is to build support among other stakeholders. It is not safe to assume that legal's e-discovery woes, for example, will appeal to HR. Fortunately, effective information governance programs provide a win for nearly all stakeholders. Hence, the key to launching these programs is often messaging the win for others.

For example, a sales group may bristle at having their email stored or being expected to properly file their electronic documents. This is the perfect opportunity to suggest ways in which good practices can protect them. Having a complete record of email communication or contract revisions can help prove ownership of responsibility for a certain promise made to a customer, protecting their relationships and reputations. This same thought process works for many individuals—good records management practices protect their interests just as much as those of the entire organization.

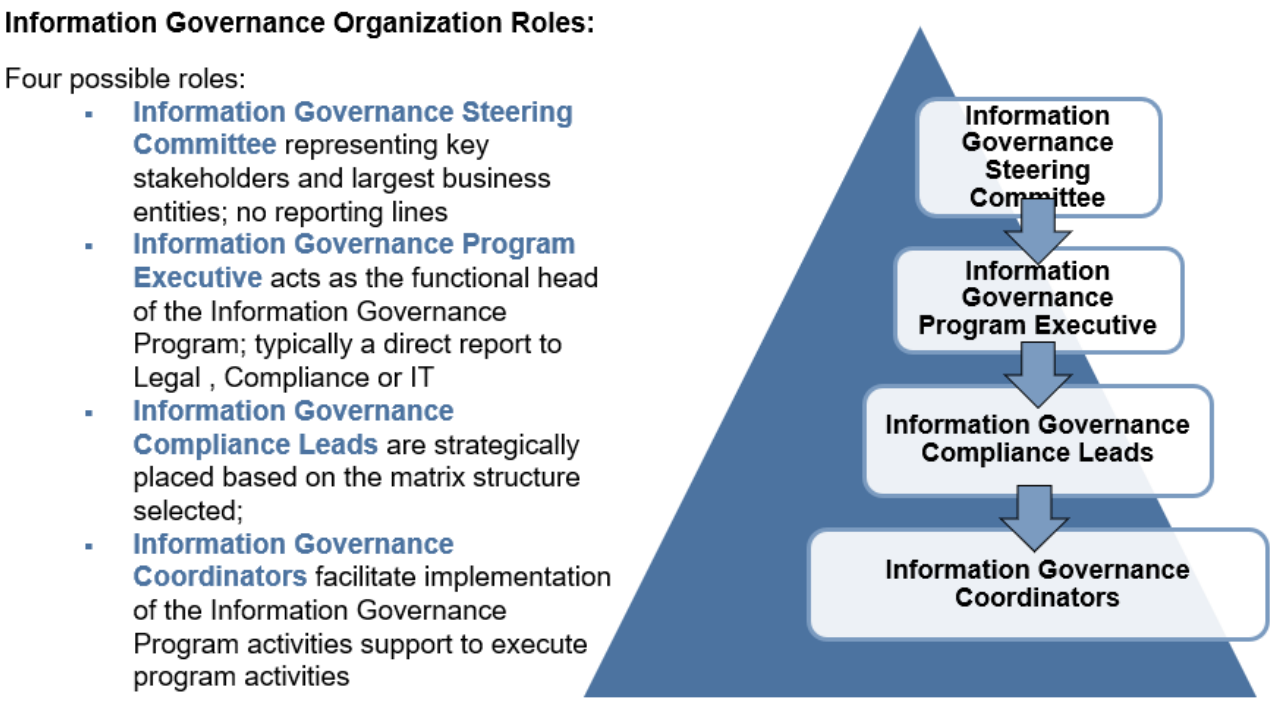
Good information governance means the organization stores less paper, thereby enabling easier compliance. Retention policies are applied as appropriate, and anything not needed to promote compliance with pertinent legal and regulatory mandates—such as those spelled out in the U.S. Federal Rules of Civil Procedure, Federal Sentencing Guidelines, Health Insurance Portability and Accountability Act, ISO standards, payment card industry, and data security standard, to name a few—is removed.

- **Protecting sensitive information**: With guidelines for proper management, it is easier to secure what must be protected, such as personally identifiable information, trade secrets, and other types of corporate confidential data.
- **Reducing storage and operational costs**: IT can centralize the control of information deletion to defer or avoid expenditures and improve application performance.
- **Optimizing e-discovery**: Control can be asserted over information before the next legal action and repeatable and predictable legal hold processes can be established to minimize business disruption.

Sell the program on employee productivity benefits. Records compliance, privacy, and better discovery just come along for the ride. Shared victories also lead to a positive side effect: functional groups can develop closer and more trusting working relationships across the organization. Each group can rightly claim its role as an enabler of, and not an obstacle to, overall business progress, and the legal department will be viewed as helping drive the business forward.

Perhaps the biggest "win" will derive from better employee productivity and enhanced collaboration. Employees can search and locate what they need to improve their job performance by reducing the time they spend in personal information management (saving and searching for email, files, and other information). In addition, when a project is finished, an employee leaves, or a group is disbanded, information that may otherwise be isolated on desktops or in personal repositories can still be leveraged for future business value.

Figure 1: The roles of information governance



Tactics for overcoming internal political barriers

Perhaps the largest challenge for combining records management and privacy programs is not legal or technical but rather organizational. If records management and privacy already exist as separate organizations, getting both groups to agree on merging into a single organization can be challenging. Key messages should be targeted separately for senior management and members of the individual teams.

Effective messages to senior management can include:

- **Economy of scale cost-effectiveness, cost reductions, and stronger returns on investment**: Records management and privacy employ many of the same processes effectively against the same corporate information. Combing both allows an economy of scale.
- **Risk reductions**: Misaligned record and privacy processes run the risk of deleting information that has a legal retention requirement; likewise, to minimize the risk of premature deletion, records may be over-retained, which poses a significant privacy risk. Combined or at least coordinated efforts reduce this risk through established harmonization.
- **Better leverage technology investments**: Technology for identifying, classifying, managing, and disposing of personal information can often also be used for similar records management purposes. Taking a more holistic view can better leverage and optimize these investments.

Final thoughts

The roles of compliance, risk reduction, information management, and employee productivity stretch across many different groups within a company. Yet, no single group is responsible for all these areas. Most information governance programs are initially organized by compliance. Why? One could argue that compliance feels the pain

of poor information management more than most departments. While this is true, we would like to offer an alternative explanation. Perhaps more than any other group, compliance has an eye on the future, navigating risks, engaging multiple stakeholders, and helping companies rise to prominence and be smarter than they were in the past. In-house compliance professionals realize that a strong information governance program not only reduces risks and costs but, perhaps more importantly, produces and enhances business value.

Takeaways

- While many see the benefit of a comprehensive information governance program, the unaddressed question of who should pay can stall program development.
- Compliance should take an active leadership role in the development of an information governance program.
- The first step in creating a program is developing a steering committee.
- The steering committee should engage business units.
- Effective messaging can help overcome political barriers in starting up a program.

1 Mark Diamond, "Who should own records management? Part 1," *CEP Magazine* (November 2023), https://compliancecosmos.org/who-should-own-records-management-part-1.