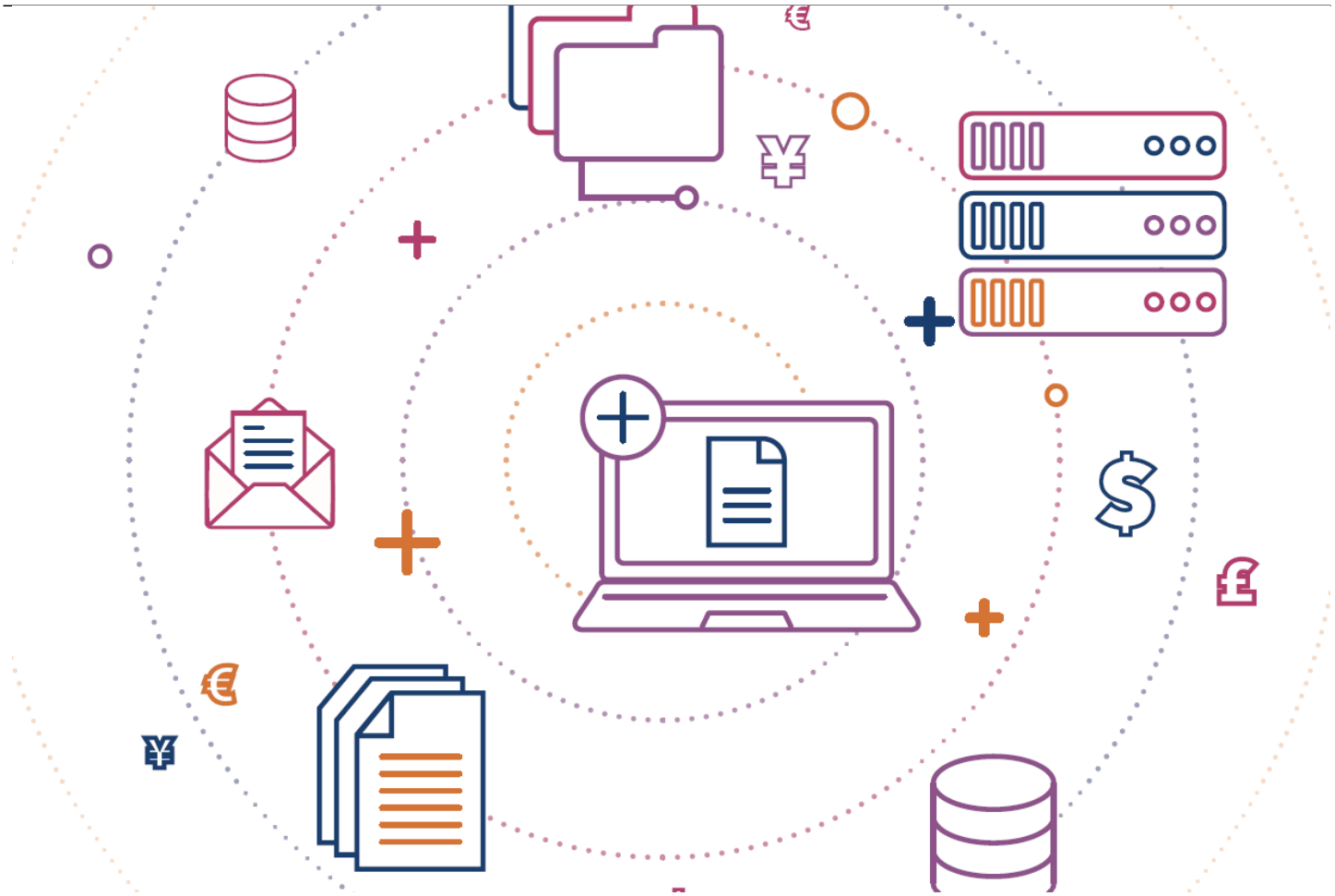
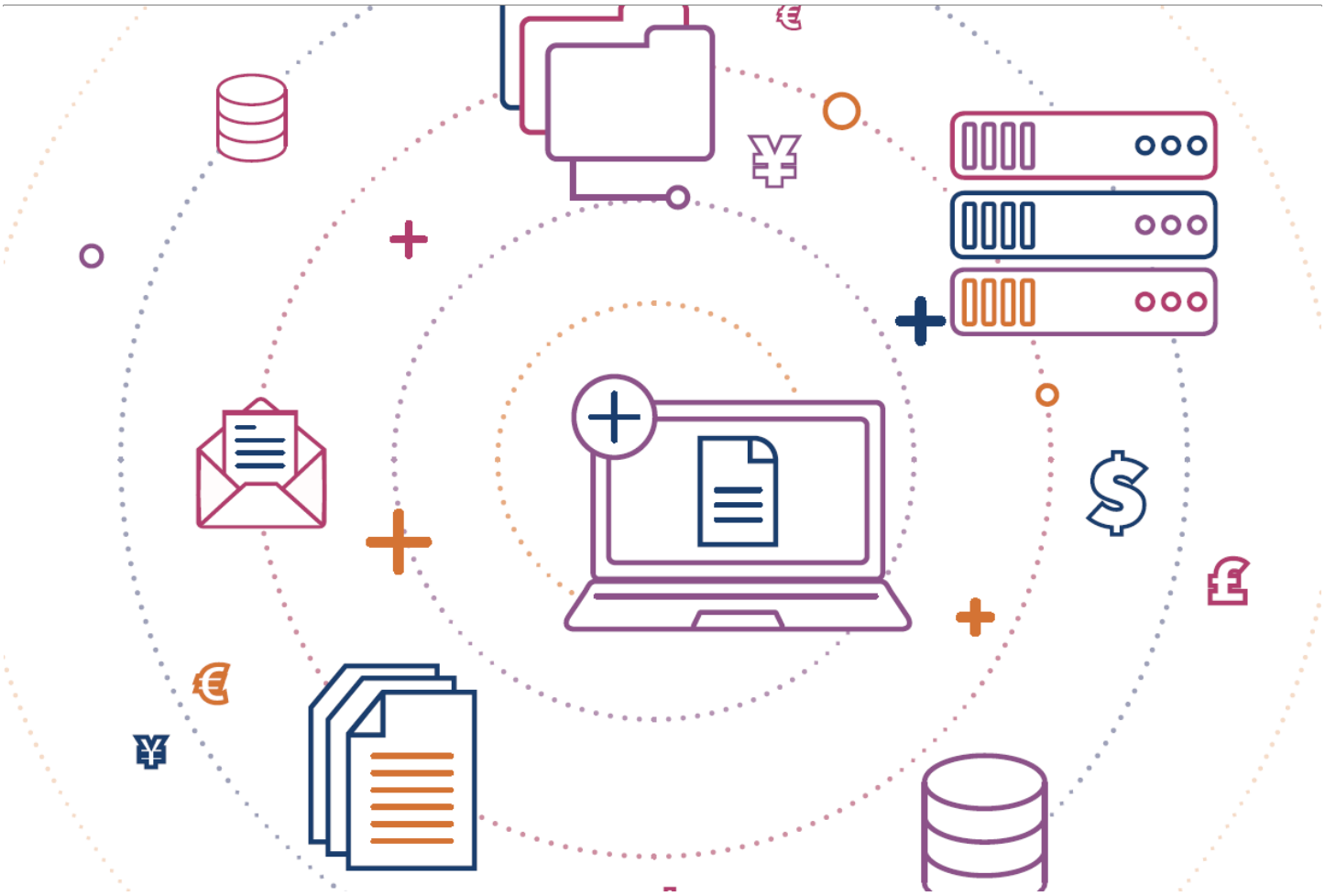
ACC DOCKET
INFORMED. INDISPENSABLE. IN-HOUSE.

Everybody's Job, Nobody's Job: The Best Way to Create an Information Governance Program Without Going Crazy

Information Governance





CHEAT SHEET

- ***Digital v. paper.*** More than 95 percent of the information a company receives is in electronic format, leading to compliance gaps when record retention programs are paper-centric.
- ***Information governance.*** Information governance is a formal discipline that holistically incorporates activities around records management, eDiscovery, privacy, security, defensible disposition, and employee productivity so that organizations can better manage, retain, secure, make available, and dispose of information through cross-functional initiatives.
- ***Key attributes.*** Common key attributes of most information governance initiatives include: combining legal and regulatory requirements with employee behaviors and business needs; focusing on measurable, practical execution; and taking advantage of technology.
- ***Program ownership.*** A cross-functional steering committee, where each stakeholder remains responsible for its area of expertise but tasks are accomplished through an integrated and coordinated plan, is the most common approach to information governance program ownership.

Compliance and data risks are hitting companies from all sides. New and expanded legal and regulatory recordkeeping regulations require more records to be retained in many cases for longer

periods. At the same time, European and new US state privacy requirements penalize companies for over-retention or improper protection of privacy information. This is occurring in an environment where many employees seemingly want to save all their emails, files, and other electronic information forever, which increases data storage burdens, cost of discovery, and information security risks as hackers continue to target these large stores of information. Finally, many companies have so much electronic information everywhere that they risk not only being non-compliant with both internal and external recordkeeping obligations, but so disorganized that employees can't find the information they need amongst the clutter.

In response, many companies are launching comprehensive information governance programs. These initiatives combine previously "siloed" records management, eDiscovery, privacy, and other information security programs into a coordinated program with single workstreams that address multiple drivers. Rising to the need, in-house counsel are partnering with information technology, compliance, privacy, and business units to reduce risks and costs, as well as to enable better employee productivity and business decision-making. Smart in-house counsel are leading, but not owning, these efforts by organizing key stakeholders to launch information governance programs.

Old information management approaches are not working

Most companies have traditional records management practices, encompassing eDiscovery, privacy, and information security programs. Yet, in today's environment, the traditional approaches taken by these programs as a whole, and separately, fall short in three distinct ways. First, many traditional compliance programs rely heavily on manual employee processes. For example, many records programs assume that most information is paper-based, 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 percent of the information a company receives is in electronic format. 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.

Second, standalone compliance programs can, and increasingly do, conflict with one another. Unless coordinated and integrated, these programs can easily conflict with one another.

For example:

- Records management that involves minimal data retention can conflict with European and US privacy requirements for maximum retention of privacy information.
- Legal hold preservation obligations can be undermined by records retention processes that require ongoing deletion.
- Intellectual property management may be undermined by eDiscovery data cleanup projects that inadvertently delete what in the past might be considered "working" or "draft" files and emails that otherwise are necessary to document the organic development of IP.
- IT outsourcing of data storage to cloud providers may run afoul of country-specific data residency regulations.
- Records management, defensible purge, and legal hold processes being undermined by employee "underground archiving," such as saving information on desktops, USB drives, home systems, or other unauthorized repositories.

This failure to coordinate standalone programs with other compliance requirements can grind work to a halt.

Third, 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 at some point in the future that they may need this information, many employees adopt a “keep everything forever” approach, saving this information on the desktops, within file shares, or email within offline PST files (“PTS” stands for Personal Storage Table, but it is mostly known by its acronym). While almost everything gets saved, most of this hidden information is actually of little value or useless — called redundant, obsolete, and trivial (ROT) data. Nonetheless, with everything saved, documents and data continue to accumulate into large electronic mountains of information. If individual employees think they must have access to their own collection of files and emails, this information is not easily shared within or across departments. Employees who believe they need to save everything get caught in a trap of their own design (or lack of design) and find it is difficult to find valuable or relevant information within the clutter. 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 ROT. Poor information management ends up being a significant drain on employee productivity.

Companies are upgrading existing functions into single information governance programs

Companies are either coordinating, or in some cases combining, multiple information management programs into integrated information governance programs. Information governance is a formal discipline that takes previously disparate activities around records management, eDiscovery, privacy, security, defensible disposition, and employee productivity and incorporates them into a holistic structure that allows organizations to better manage, retain, secure, make available, and dispose of information through cross-functional initiatives. Through purposeful collaboration amongst these activities, companies are reducing costs, lowering risk in litigation, increasing compliance, and perhaps most importantly, making their employees more productive.

No two information governance programs will necessarily be the same, as each company has its unique combination of compliance requirements, litigation profile, business needs, and company culture. That said, common key attributes of most information governance initiatives include:

- A combination of techniques to combine legal and regulatory requirements with employee behaviors and business needs;
- A very strong focus on measurable, practical execution; and
- Intelligent use of technology.

Three methods for management of electronic information

A characteristic nearly all successful information compliance projects share is the ability to apply governance controls to information. These controls include retention, information security, search, and access. While there are many methods to apply these controls, they generally fall into two categories: manual processes and data placement.

Manual Process

Manual processes involve employees sorting through all of the documents and tagging, classifying, and (one hopes) storing a copy in the correct repository. These processes usually include employees looking up the retention period for any given record or document or applying data security tags to a

document from a drop-down menu.

In general, taking a manual approach to applying information governance for electronic information does not work very well.

- First, desktops, file shares, email, PST files, and other places employees store information lack effective information security protocols, access controls, or easy-to-use search capabilities.
- Second, manual processes bump up against the “five-second rule.” If it takes an employee longer than five seconds to identify, classify, and store information, most employees will blow it off, or try to shortcut the process. Researching record retention requirements within a larger policy, determining data security classifications, and tagging files and emails often take much longer than five seconds.
- Manual classification works a little better in a world of paper, but the sheer volume of the electronic documents that employees touch each day has led many companies to adopt an easier-to-execute data placement strategy.

Does the California Consumer Privacy Act require information governance?

California Consumer Privacy Act (CCPA) enforcement is likely to begin in mid-2020. While the act itself does not specifically require companies to have an information governance program, practically speaking compliance will be difficult to achieve without one. CCPA requires organizations to secure, identify, produce, and delete privacy information. This must be coordinated with records retention and legal hold obligations. Likewise, these functions must be implemented across a variety of media, including data stored in databases, emails, and files. More than 80 percent of the tasks required to comply with CCPA are traditional information governance functions.

Data placement

A data placement strategy combines both policy with technology to make records and document classification both faster and easier. First, a number of records and document repositories are made available to employees. These could be content management systems such as OpenText, a cloud-based offering such as Microsoft’s Office365, or a contract management application. Most organizations use a variety of repositories to hold different types of documents.

Second, each repository is configured with appropriate folders to hold different record types for various departments. This folder hierarchy is called a taxonomy. Each folder in each repository is configured with retention and other governance rules matching, for example, the requirements outlined in the retention schedule. Most systems can be programmed so that when a user places a file in one of these folders, the system will retain it for a specified period (five years, for example) and then, assuming no legal holds are in place, the program will automatically delete the record upon expiration of its retention period. This configuration is not limited solely to retention. Systems can be programmed to automatically tag each record or document according to its proper data security classification, access controls, and collaboration features. These documents could then easily be sorted and retrieved whenever necessary.

Across the enterprise, there may be multiple repositories, and within each repository, there may be many folders. However, making every repository and every single folder available to all users might be too overwhelming. Rather, these systems have the capability of showing users the three or four places their records and documents live. When properly configured, users need only put their information in the right place, and these systems will enforce all the rules.

If this sounds complicated, that's because it is, but it is also manageable and achievable with sufficient planning and the right tools. Determining which files and emails go in which repositories, and mapping the retention schedule and other policies against the folders, can be quite complex. The overall goal of this approach is to move the complexity away from the user and move it into the system itself.

Record and document retention for employees should be fast, intuitive, and easy. A data placement strategy works because it's simple, fast, and easy enough that employees are much more likely to use it over their own haphazard "systems." Another advantage is that it kills multiple compliance birds with a single stone: Electronic repositories can be programmed not only to tag documents for retention periods but also for data security classification, collaboration, access controls, and even legal holds.

Information governance case studies

CASE STUDY #1: A HEALTH INSURANCE ORGANIZATION CLASSIFIES AND DELETES EMAIL

Information problem: A health insurance provider needed to get better control of emails as, for many years, employees had adopted a de facto "save everything" policy, storing their emails in their own personal folders. These emails contained a variety of active records, privacy information, corporate confidential data, as well as significant amounts of low business value or expired information. In addition to the security risks, the ongoing accumulation of this data significantly increased discovery costs and was burdensome during regulatory inquiries.

Information governance projects: The company embarked on a multiple-month email policy and archiving project that included email policy updates, technology acquisition, employee training, behavior change management, and audit programs.

Impact: Emails that were records or had sensitive information were properly classified and more than 45 million emails were defensibly deleted during the pilot — all with no employee complaints.

CASE STUDY #2: A GLOBAL MANUFACTURER MANAGES AND PROTECTS INTELLECTUAL PROPERTY

Information problem: A global manufacturer was concerned about securing and managing its intellectual property (IP), much of which resided in computer files stored on file shares and employee desktop systems in its offices throughout the world. In light of data breaches perpetrated by overseas entities, the board of directors' audit committee raised concerns about managing and securing this information.

Information governance projects: The company first updated its data security classification policy, making it both simpler — describing what types of data needed to be secured, how, and for how long — and more comprehensive. It then implemented a data placement strategy, defining appropriate

repositories for all types of information, with appropriate security controls, such as passwords. Once these were in place, both new documents as well as older information were stored and secured.

Impact: Previously, only 15 percent of the company's IP was managed in accordance with the data security classification policy. After this initiative, subsequent audits revealed that 85 percent of the information was being managed appropriately. Over time, the company continues to address the remaining 15 percent.

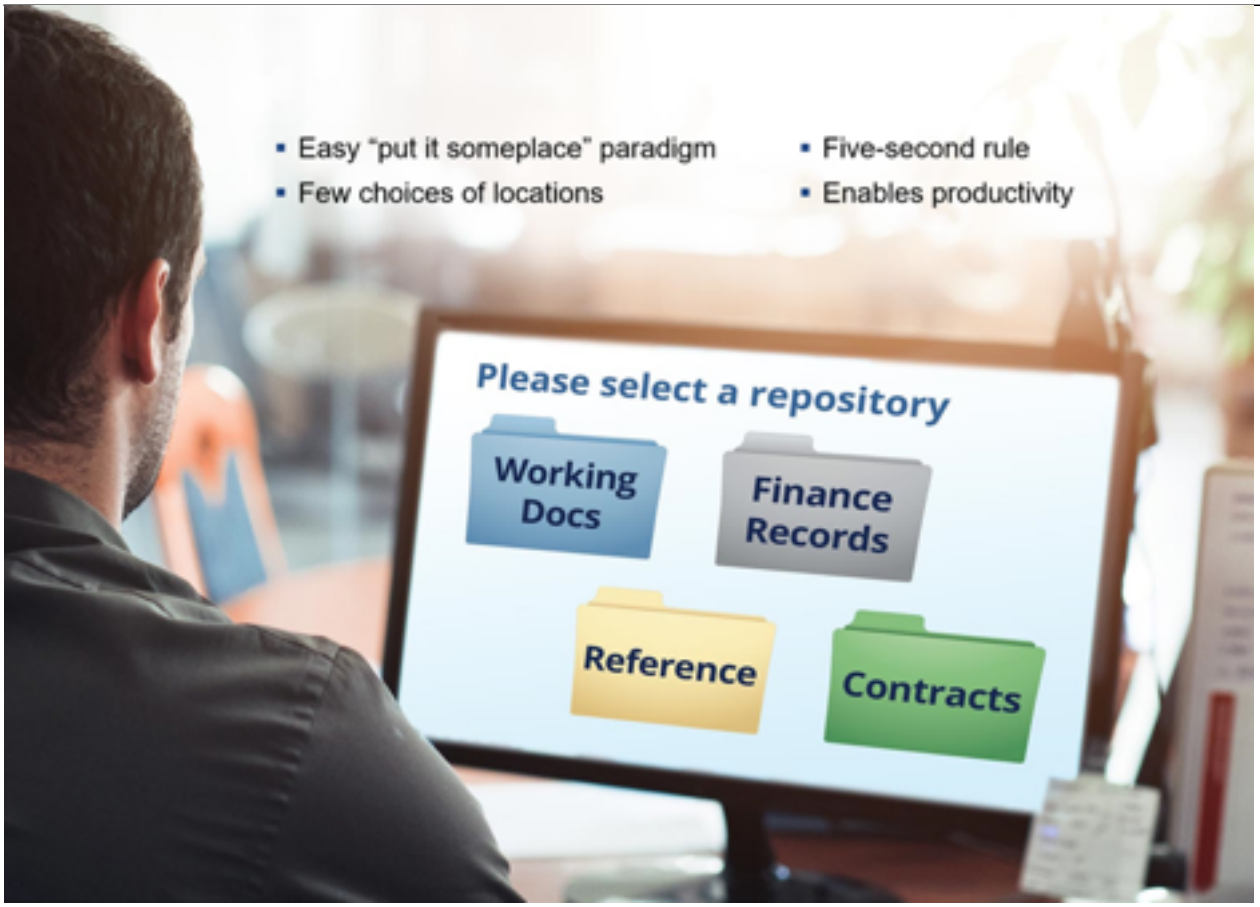
CASE STUDY #3: LIFE SCIENCES COMPANY DRIVES EMPLOYEE INNOVATION THROUGH BETTER RECORDS MANAGEMENT

Information problem: Through a series of acquisitions, the retention and disposition processes for a mid-sized life sciences company had become disjointed. While this raised compliance concerns within the legal department, senior management was more concerned with increasing employee innovation and collaboration, especially across the newly acquired business units.

Information governance projects: In a ground-breaking move for this company, the legal department partnered with IT and rebranded their records program as an employee innovation program. They conducted an information inventory, updated their record policies, and mapped what data lived where. They used this information when they moved to a new, company-wide document management system.

Impact: They were able to identify significant amounts of duplicate information, as well as content that needed to be made more accessible across the organization. Users were encouraged to better collaborate, and controls were put in place to better manage and delete obsolete or outdated content.

Data placement strategy from an employee's perspective (1)



Can autoclassification technology just give us an “easy button”?

An emerging method for applying records management and other compliance to information is leveraging technology to “autoclassify” information. Today, computers can be taught through an iterative process to recognize a document type by its content, and automatically classify it according to its instructions. This is most often used in eDiscovery through technology-assisted review to sort relevant from non-relevant documents. Theoretically, the same technology can be used to apply records retention, data security classification, and other governance. This technology holds great promise and will drive records management in the future. However, in our view, these technologies are not yet fully mature and expectations might need to be tempered. Records classification is often magnitudes more complex than the discovery associated with a single legal matter. Furthermore, the case law supporting record types by true autoclassification — without any human involvement — is lacking. However, all is not lost. Autoclassification can do a fairly good job identifying certain types of specific information, such as personally identifiable information (PII) and protected health information (PHI) for privacy or searching through a series of contracts looking for a particular term. They can also successfully identify low-value or outdated information that should be deleted.

Defensible disposition of unneeded files and emails

Organizations should routinely delete unnecessary information. Such information can clog a

computer system’s operation, take up memory, create confusion if there are multiple versions, and in some cases, increase vulnerability to hackers and competitors. Making disposition repeatable and consistent are the pillars of a defensible information governance program. For those struggling with a defensible disposition protocol, a sensible starting point is to form a cross-functional team to examine current information management and legal response processes. Once this team is able to identify the business “pain,” it can demonstrate in a specific fashion how defensible disposition and managed retention programs will yield measurable benefits for all users. This team will be able to consider “hard” cost savings, such as postponing storage expenditures, as well as “soft” cost savings, such as reducing the amount of time spent by employees searching for information or working through litigation holds.

Cleaning paper record storage

While much of the focus on information governance is on electronic information, many companies are still burdened with legacy paper records — sometimes warehouses full of paper archives. Over-retained records (and other non-record, or copies of documents, and other extraneous materials) result in higher cost beyond that charged by offsite storage vendors (which in itself can be extremely expensive). For example, paper records are subject to discovery. In the event of a lawsuit or request from regulators, these discovery costs can be costly, but they can be reduced by decreasing the amount of paper that must be searched.

Paper disposition often follows the same steps as electronic information:

- First, establish your policies to include an up-to-date records retention schedule and legal hold process.
- Next, identify the locations of paper records. Companies are often surprised by where these boxes are being stored.
- Then develop a repeatable, documented process for classifying these records. Everything outside of the retention policy and not under legal hold can go. Have faith in your process. Paper records often have an advantage in that they are stored in a location that is not easily accessible by employees. Thus, paper records disposition often requires much less “buy-in” from the employees and business units.

Data placement strategy from an employee’s perspective (2)

- Easy "put it someplace" paradigm
- Few choices of locations
- Five-second rule
- Enables productivity

How can we get employees to follow our policies and processes?

How and where employees save files, emails, and other information is often a deeply ingrained behavior. Getting them to change that behavior by saving their information in a different place, through a specific process, is often the most overlooked yet essential element of an information governance program. While many supervisors have the authority to mandate information management policies and processes, getting employees to actually follow them requires employee behavior change management.

Behavior change management is a formal discipline that includes messaging, communication, training, and audit. It may be tempting to tout the compliance benefits to the company of a program to employees. But selling the enhanced productivity “wins” is much more likely to change employee behavior and foster program compliance.

From an employee’s perspective, one may ask how no longer “saving everything forever” and instead taking a “save the right information in the right place” approach is a “win” for employees. Dig a little deeper and one can find huge, meaningful wins. Well-designed information governance programs avoid frustration and make individual employees more productive in that:

- Employees can quickly find information;
- It’s easier to share information within and across departments;
- Their information is more accessible and therefore they may not need to bring their laptop with them home or on vacation; and
- Whenever there is turnover, the previous employee’s work is now readily available.

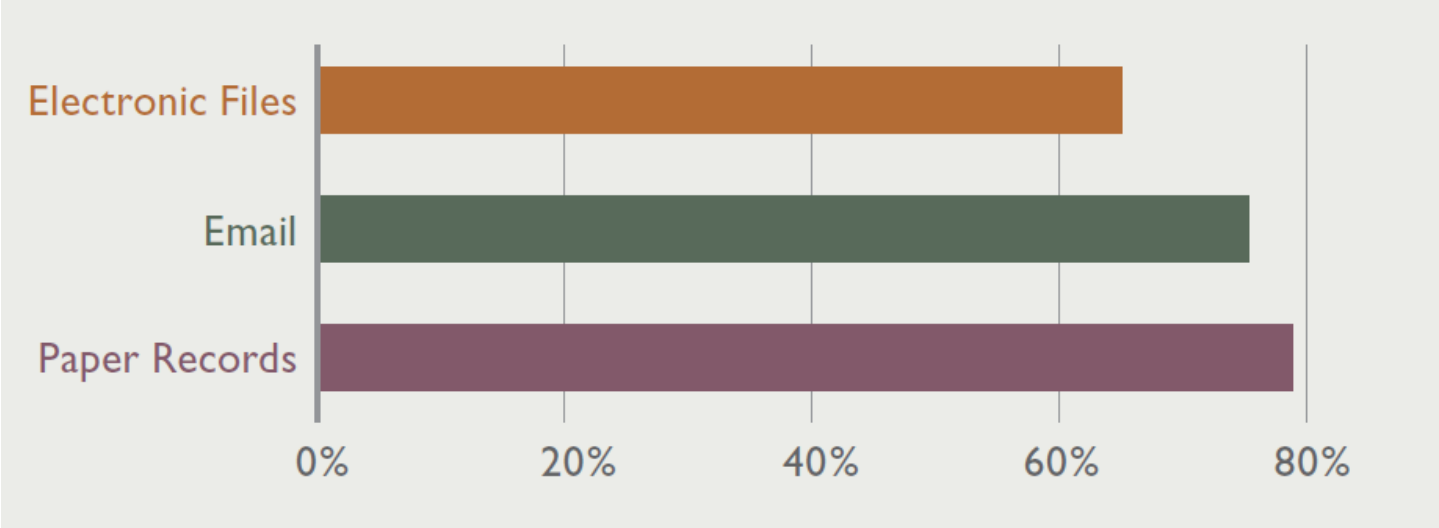
There can still be consequences for poor or unsafe information management practices, but when launching a new program, start with the wins.

Avoiding underground archiving

Most in-house counsel don’t like email. If litigation looms, they believe that the more old emails a company has, the more likely a “smoking gun” will emerge in discovery. Therefore, it is not surprising that many companies are taking active steps to delete emails early before they can do harm. The most common deletion technique is “aggressively” deleting any emails older than 60 or 90 days directly from the employees’ email boxes on the email server. Although well intentioned, these aggressive email deletion strategies can backfire, driving employees to “underground archiving,” where, in a bid to save their emails from deletion, they save emails on desktops, laptops, centralized file servers, USB drives, and other unauthorized areas.

Companies can respond to these underground archiving practices by shutting down the ability to use USB drives (generally a good practice). Through a data placement strategy coupled with effective employee education and resulting behavior change, management in many companies have deleted large amounts of emails — without driving underground archiving.

Disposition Targets



Average percentage of expired records and low-business-value information that can be deleted while maintaining compliance and retaining information still needed by the business.

Who should run an information governance program — legal or IT?

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

Single department ownership

Traditional programs are owned by a single group, such as the legal department. While elements of an information governance program, such as policy development, may be owned by the legal department, information governance requires a broad skill set. Therefore, very few programs are owned solely by legal, IT, or by another single department.

Chief information governance officer is responsible for multiple functions

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. 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

By far the most common approach when launching an information governance initiative is to create a cross-functional committee composed of multiple stakeholders. Typical committee members include legal, IT, compliance, 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. The vast majority of companies with successful information governance programs take this type of cross-functional approach.

Final thoughts

The biggest challenge with information governance is that it is everybody's job and also nobody's job. 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 the legal department. Why? One could argue that legal feels the pain of poor information management more than most departments. While this is true, an alternative explanation is that perhaps more than any other group, legal has an eye on the future and is skilled at navigating risks, engaging multiple stakeholders, and helping companies rise to prominence and be smarter than they were in the past. In-house counsel realize that a strong information governance program not only reduces risks and costs, but perhaps more importantly, produces and enhances business value.

Patrick Chavez

Chief Privacy Officer

Edward Jones

He also has responsibilities as an associate general counsel leading the Records and Information Management Program within the legal division. Chavez is a member of the International Association of Privacy Professionals and has earned the organization’s Information Governance Professional certification.

Mark Diamond

CEO and Founder

Contoural Inc.

Mark Diamond is the CEO and founder of Contoural Inc., an independent provider of information governance consulting services. His company works with more than 30 percent of the Fortune 500, plus many mid-sized and smaller companies.