ACC Association of Corporate Counsel

ACC Guide^{SM}

Automating Your Records Management Program

Sponsored by:

contoural

Automating Your Records Management Program

August 2020

Provided by the Association of Corporate Counsel
1001 G Street NW, Suite 300W
Washington, DC 20001 USA
tel +1 202.293.4103
fax +1 202.293.4107
www.acc.com

This ACC Guide[SM] addresses global strategies for automating elements of a records management program. In today's environment of electronic information, manual record management processes cannot keep pace with the sheer volume of electronic information being created and received. Companies need to automate their record processes for the identification, classification, update, and disposition of this information. Much of this automation can be accomplished with technology companies already own today.

This material was developed by Contoural, Inc. Contoural is a sponsor of the Information Governance Network and a sponsor of the Legal Operations Network Records Management and Information Governance Foundational Toolkit. For more information about the author, visit their website at www.contoural.com or see the "About the Company" section of this document.

Contoural and ACC wish to thank members of the Information Governance Network for their support in the development of this Guide.

The information in this ACC Guide should not be construed as legal advice or legal opinion on specific facts, and should not be considered representative of the views of Contoural, Inc. or of the Association of Corporate Counsel (ACC) or any of its lawyers, unless so stated. This ACC Guide is not intended as a definitive statement on the subject, but rather to serve as a resource providing practical information to the reader.

This publication is independent from, and is neither affiliated with, nor authorized, sponsored, or approved by, Microsoft Corporation.

Contents

I.   Introduction

Records management execution is a source of frustration for many companies. They find it difficult to get their employees to consistently follow records management procedures, especially for newer electronic information. Paper records are filling up record storage facilities and files, emails and other types of electronic information are overwhelming data storage systems. At the same time, the legal and regulatory recordkeeping environment is becoming stricter. New stringent privacy rules require that personal information be identified and deleted when no longer needed or upon request. Making these challenges worse, employees tend to hoard documents, convinced that they need to save everything forever. Left unaddressed these problems only get worse, making records compliance even harder.

To face these challenges, modern records management approaches coupled with newer technology (much of which companies already own) can simplify and automate records management processes. These smart strategies make the entire process of identifying, classifying, retaining, retrieving, and disposing records and other information easier. These automated approaches can move you from a state of frustration to a state of compliant execution.

II.   The Challenge and Despair of Managing Electronic Records

While companies continue to accumulate large stores of paper records, most often the root of their record management problems lie in the management of electronic information. According to Association of Records Managers and Administrators (ARMA), more than 95% of an organization's information is received or created in electronic format, and 90% of paper information is sourced electronically. Traditionally, records retention programs were designed for the retention and disposition of "official" paper records. Program execution came down to sorting the right paper into record storage boxes, and (sometimes) destroying those boxes once their retention period expired. Yet, as companies move into the digital age, their records management practices have not kept pace.

A. Frustration That Employees Will Not Follow Records Management Procedures

Traditional records management classification, storage processes and procedures require employees to take time-consuming steps. While these manual steps may only take 60 seconds, multiplied against the hundreds of records employees may receive or create each week, those 60 seconds can potentially equal hours of records management burden. Adding to the time burden, many companies have set up complicated records taxonomies and file plans, discussed below, and employees cannot easily determine the correct place to store records. The fear among some employees is that if they put their files into a records management system or other type of repository, they may not be able to find this information again.

Contoural's Five Second Rule
The average employee sends and receives 167 emails and more than 25 files each day. We find that employees will spend at most five seconds manually classifying a single document, and even that short period of time works out to more than an hour per week, per employee to classify information. If the manual records classification and management process takes longer, even well-meaning employees will soon start ignoring the process. Manual classification worked 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 data placement strategy.

Records progam managers looking for compliance support from their business units may receive little or none. These business units believe that records compliance is "the legal department's problem" and while providing superficial support for a program, they do little to actively encourage their employees to comply. They do not see the connection between good information management practices and the business benefits accrued to their division or its employees.

B. Some Companies Have Effectively Given up Trying to Manage Electronic Information

The result of this noncompliance is that electronic information simply accumulates. Most companies have a significant amount of *R*edundant, *O*bsolete and *T*rivial information (ROT) – expired records, copies of information, or simply information that has low or no business value. This ROT is often identified as an issue during eDiscovery, as it increases the costs and risks of litigation.
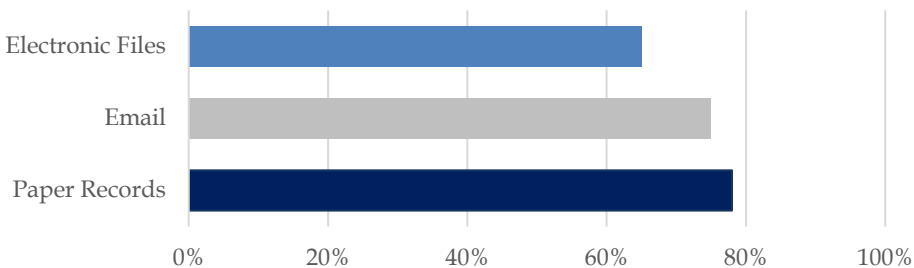
Figure 1. Average percentage of expired records and low-business-value information that can be deleted while maintaining compliance and retaining information still needed by the business. Source: Contoural, Inc.

Perhaps more worrisome is the emergence of new, global privacy laws. These laws require that personal information be classified and retained only for legitimate business purposes and then deleted. Most privacy laws also permit a data subject to request his information be deleted. Many traditional records programs have taken refuge in the idea that while they significantly over retain electronic information, as least they are compliant with recordkeeping minimum retention requirements. Yet these privacy laws are declaring that saving personal information – typically intermixed with all the other content – for long periods of time is decidely noncompliant. Poor records management practices are colliding headfirst into these new privacy rules.

It is time to rethink the approach. If the advent of computers brought companies into this records management mess, perhaps they can help us find a way out of it.

III. Automation Strategies to Avoid and Practices That Do Not Work

Effective automation is the trail leading out of the records program morass. Yet as not all trails lead you to where you want to go, not all automation strategies drive better compliance and information management. Some automation strategies – while seemingly easier and well-intended – lead us down the wrong path. We explore these ineffective strategies first.

A. Perpetually Updating Schedules – Easier Now, Harder Later

Legal and regulatory recordkeeping requirements change periodically. These changes can be country-specific, at the local, state, or provincial level, or may occur as part of new or updated industry-specific regulation. Records managers need to keep abreast of these changes to ensure that they are following the latest regulations.

One approach that has emerged over the past five years is to utilize a web-based technology that permits schedules to be managed and automatically updated online as laws and regulations change.

These cloud-based schedules, created by large tech firms and service providers, operate under the idea of identifying all regulatory changes as they occur, and then dynamically updating the retention period in a company's schedule. At first, this seems like a great idea. Unfortunately, while they make a small part of the records program easier, they drive larger compliance gaps.
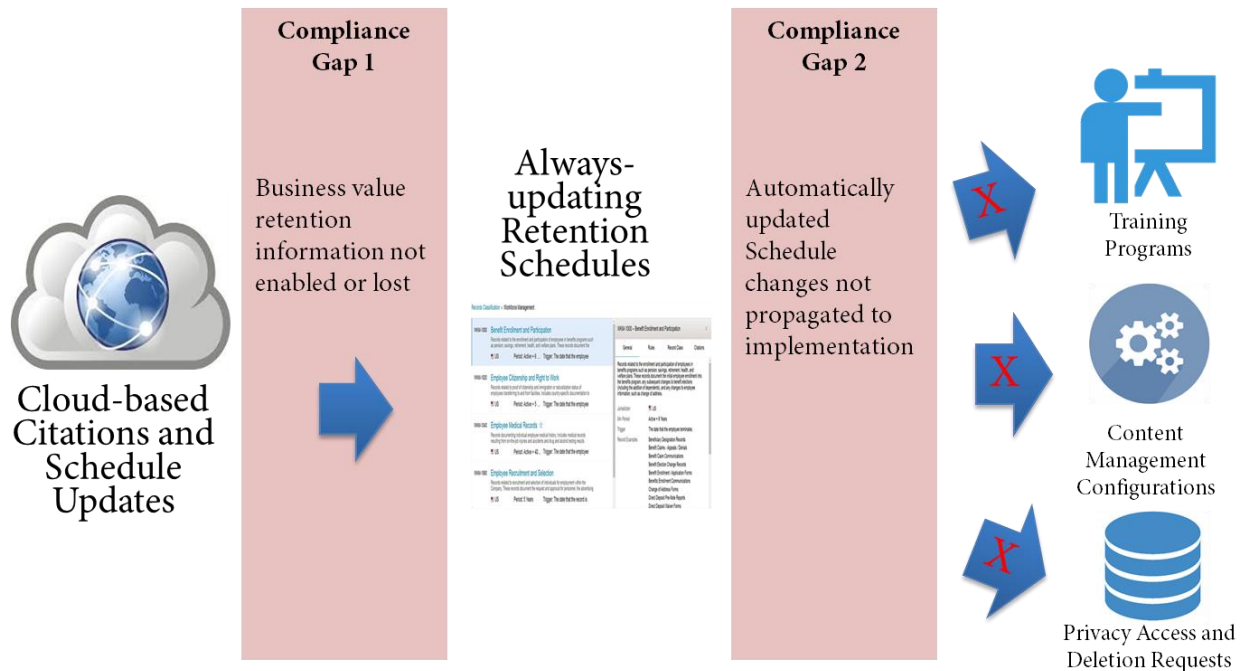
The main problem is that these perpetually updating schedules are not synchronized with program execution. If a schedule gets updated every week, a company in turn would also need to update their records processes and training every week. As soon as a company's policy changes, records processes, training and configurations should also be updated concurrently. Since an online schedule can potentially change on any given day, companies are not prepared to update their execution process as quickly. This in turn creates a compliance gap between policy and implementation.

This is important for compliance. Regulators are looking for, and regulatory compliance comes from, companies' ability to demonstrate they are following their policies. They are typically less concerned that the policy contains the latest change in regulatory requirements (nearly all these regulatory changes provide a grace period of quarters or even years), and much more concerned about companies executing their policies.

This cloud-based approach also assumes that the schedule is based exclusively on legal and regulatory requirements, which should not be the case, as is explained further in the next section.

Companies should avoid having gaps between what they say they will do – per their policy and schedule – and what they are actually doing as reflected in their training programs and processes. Any differences between the two have will be exploited by regulators and litigators as bad faith implementation of policy. A better practice is to schedule periodic refreshes of the records policies and schedules at one year or eighteen-month intervals, for example, and capture any regulatory changes during this update. Then concurrently update training, processes, and configurations. As discussed below, these steps can be automated. Compliance is best achieved by having a tight coupling between policy and schedule with actual practices.

B. Complex and Detailed Taxonomies Make Employees Frustrated

A common lament among records managers and their IT counterparts is that they have configured information repositories (such as Microsoft's SharePoint product) but cannot get employees to store their records and other information in these systems. The problem may not be the employees, but rather how these sites have been set up as overly complex.
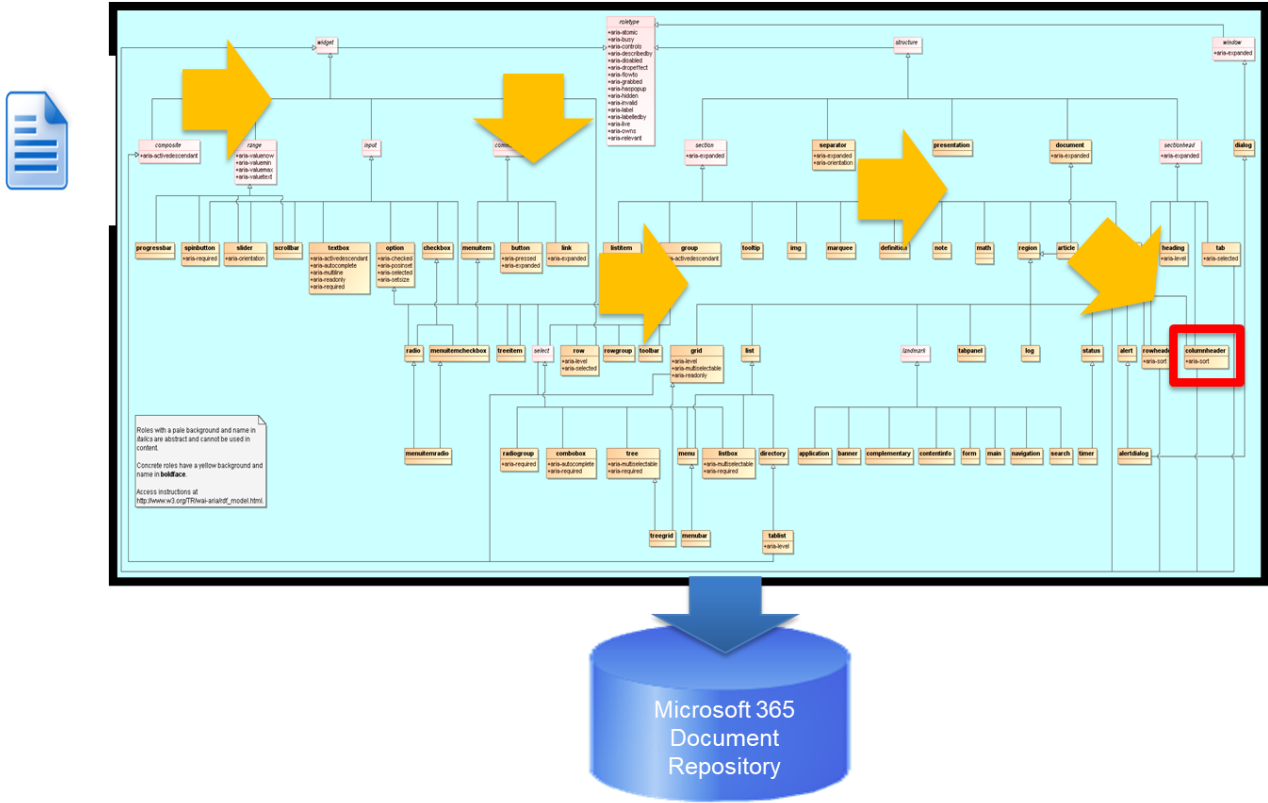

Figure 3. If employees need to navigate overly complex taxonomies and file plans to store their documents, they will find it difficult and simply store their information someplace easier. In the example above, employees need to navigate several directories and levels to store their documents in the correct folder. Source: Contoural, Inc.

Realizing that different retention periods not only apply to different documents, but also layer on top of retention, privacy, data security and other governance requirements, a common mistake is to get "taxonomy happy" - creating detailed and complex taxonomies or directory structures. While these complex structures may seem appropriate and reasonable to a records manager or enterprise content professional, they are found to be difficult by most employees for being too complicated and cumbersome. This navigation process greatly exceeds the "five second rule" discussed above. Furthermore, employees fear that even if they store their documents in the correct folder, they will not be able to find it later. As a back-up measure, they save a copy of their documents someplace else, negating the intention of saving everything in a single place.

The corollary to complex taxonomies is having long and detailed drop-down menus, which some systems require employees use to classify documents. These drop-down menus present employees with as much as a dozen choices. The process of classifying records through these long drop-down menus becomes tedious. As employees' patience runs out, they may end up choosing the first entry on the menu as a default solution, or simply choose the longest retention period.

The problem is not the type of repository, be it SharePoint and other types of content management and record management systems. The problem is how these systems have been configured.

C. Aggressive Deletion Drives Underground Archiving

Frustration by Legal and senior management for employees' "save everything forever" mentality can boil over during a painful eDiscovery episode when, for example, Legal and IT management enable an "aggressive deletion" strategy that employs automated deletion programs across file shares and email inboxes as well as deleting older files or any emails older than 60 or 90 days. Although well intentioned, this strategy can quickly backfire.

When companies start an email deletion process, employees often react with a counter behavior of "underground archiving." In a bid to save their emails from deletion, employees save emails on desktops, laptops, centralized file servers, USB drives, and other unauthorized areas. Companies respond by shutting down the ability to use USB drives (generally a good practice). In an information retention and disposition arms race, employees start forwarding emails, and send files, or other information they believe they need, to their personal email account. Some employees have been known to create Google Gmail accounts solely for this purpose. Companies then try to tighten down on outbound emails, but employees find another way and the arms race continues.

Senior Legal and IT management is correct in its theory. Employees do save too much ROT and other unneeded content. Yet their strategy of aggressively deleting information truly doesn't work and the diaspora of email and files outside the company makes the problem worse.

D. Employee Self-Certification of Records Compliance Does Not Work

Another approach is to put the records management compliance burden entirely on employees. Some companies have adopted an employee records compliance self-certification process: an automated system sends out a link every month to employees, requiring them to click the link to confirm their compliance with the program. Those who fail or do not click the link to acknowledge their compliance with the program face disciplinary action.

Putting the compliance onus on the employees has an apparent simplicity and ease. However, many assessments of records program compliance have shown that this type of self-certification does not actually work. Employees tend to follow the process initially, but soon fall behind on declaring and retaining their records. They still click the link claiming compliance, thinking to themselves they will catch up classifying all their records and complying with the policy. They fall farther and farther behind. Over time, despite their self-certification that they are following the records program, they fall further and further out of compliance. This gap can become a major issue during a regulatory inquiry or any litigation.

E. Human-free, True Autoclassification Is Not There Yet

The pinnacle of records management is to leverage technology in which advanced computer systems analyze the content of files, emails, and other types of record-containing media, and automatically classify this content as a record, all without humans being involved. These systems are envisioned to run autonomously in the background, classifying, storing, tagging, and managing records. While true autoclassification and content analytics techology has made tremendous strides in the past decade, there are still significant limitations today on how it can be applied to records programs.

Auto-classification and content analytics technology has been driven largely in the Information Governance space by eDiscovery. These systems have demonstrated that they are more accurate and consistent than humans in identifying and classifying relevant information as part of discovery. Yet the application of the same technology for records management faces large barriers.

First, unlike eDiscovery which is focused on a single matter with a narrow set of search terms, a typical corporation may have thousands of records types across multiple media, involving tens of thousands of search terms. Automated content analytics for records classification can be much more complex.

Next, the case law supporting record types by true auto-classification – without human involvement - is lacking. Regulators have yet to give approval on classifying or not classifying a document as a record without direct human oversight. Finally, unlike eDiscovery where information is being sorted into relevant and non-relevant piles, records management has a finality associated with it: content that is classified as a record is saved, and content classified as a non-record may well be permanently deleted.

There is one area, however, where content analytics is being used successfully today. These technologies do a good job of 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 also can do an adequate job of identifying low-value information that is not required to be kept (such as expired records, non-records or duplicates) and should be deleted. Sometimes cleaning up the *r*edundant, *o*bsolete or *t*rivial data can go a long way to reducing costs and risks. However, these technologies are not the ultimate solution that some have claimed.

IV. What Needs to Be in Place Before Starting Automation

Records program automation rests on a foundation of good policies, practices, and participation. Records programs that engage a larger cross-functional team gain more traction more quickly and simplify the path to automation.
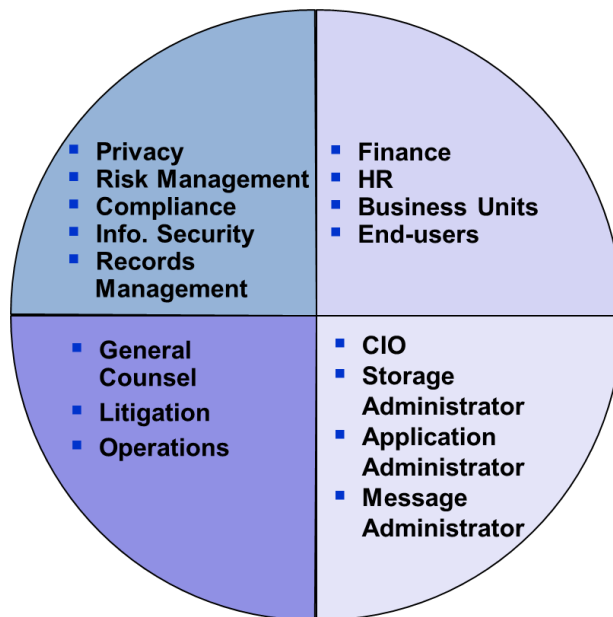
A. Create Your Cross-functional Team

Figure 4. Automating a records program should engage cross-functional stakeholders. Source: Contoural, Inc.

Automating a records program should not be attempted alone. Rather, key stakeholders from legal, IT, risk, compliance, security, privacy, records management, and especially business units should be engaged. Automating a program involves synchronizing policies, processes, technology, and training. A well-established team will be better positioned to get the job done.

B. An Up-to-date Records Retention Schedule That Is Compliant and Is a Consensus on What to Save

Note: This section summarizes important attributes of a modern schedule. A detailed overview of this is presented in the ACC Guide: "Creating Modern, Compliant and Easier-to-execute Records Retention Schedules."

Legal, IT, risk, compliance, and your business units need to agree on what to save and not save. For example, automation sometimes gives a false sense that it is not necessary to build this consensus since deletion will be automated, even over the objections of the business units. These attempts of automation without consensus usually end badly, often leading employees to engage in underground archiving, as discussed above.

A key first step is developing a modern and compliant records retention policy and schedule. At its core, a policy and schedule not only defines legal and regulatory recordkeeping requirements, but also builds consensus across key stakeholders, business units and employees, on what information has business value and should be saved, for how long, and what can and should be deleted. Good policies and schedules address both legal and regulatory requirements and business value.

Achieving consensus does not mean giving in to some employees' stated desire to "save everything, forever." Rather, it achieves a balance on retaining what is needed for business value, while separating out the low value clutter that makes finding and managing information difficult. "Save everything" employees typically only really care about a small percentage of information. In identifying this content and enabling its retention through effective records retention, everyone is freed up to delete everything else. Deleting unneeded information can feel liberating.

C.   An Updated and Defensible Legal Hold Process

Before automated deletion can commence, companies need to ensure that information under legal hold is protected. An effective hold process addresses the following requirements:

- *Hold notification* – The issuance of a litigation hold notice that lets custodians (employees and non-employees, as applicable) know of their obligation to preserve relevant information, and specifies how they should do so.

- *Information security* – To prevent the deletion, loss, or inaccessibility of relevant documents, such information needs to be saved in a repository that is separate from other information assets.

- *Ongoing preservation* – A process must be put in place to ensure that once a hold notice is served, all future relevant documents are also subject to the legal hold and are properly preserved.

- *Hold release* – Once a particular matter has been settled, and provided that future litigation is not anticipated, the organization should "release" the hold, notify custodians, and resume normal retention and disposition programs.

All these elements of the legal hold process must be supported by documented procedures, standard templates, repeatable workflows and forms (or electronic tracking and management systems), along with the appropriate training for litigation support staff, organization managers, and all other employees. Ensuring the information under preservation is properly protected, the deletion process is freed up to allow deletion without fear of spoliation.

D. Training and Behavior Change Management

Note: A detailed overview of employee behavior change management is available in the ACC Guide: "[Executing Your Records Retention Policy and Schedule](#)"

The best policies, processes, and technologies for automating records management will not be effective unless employees are engaged.

Change management, including communications and training related to this automation, is a critical element to drive user compliance. Designed to drive users toward a target behavior set and to measure progress in achieving compliance, these change management activities provide formal, consistent communications to employees and executive sponsors during implementation.

Before any information is moved or modified, it makes sense to train, explain, make resources available and even over-communicate how this will impact their access to information. Even better, any records automation strategy should endeavor to "sell" employees on how the new system or strategy will make their lives easier and more productive.

E. Do You Really Need to Buy New Technology to Automate?

Many automation strategies depend on implementing some type of software or hardware technology tool. Does this mean that companies that want to automate their records programs need to buy new technology to do so? Most often, the answer is no. Many companies today already own products that can be used to automate their records programs. A good example of this is the Microsoft 365 suite of products. Many companies have deployed Microsoft 365 (formerly known as Office 365) to move email and file management into the cloud and reduce costs. In addition to Microsoft, many companies have deployed similar types of enterprise content management systems. However, while many companies already own these types of tools, most companies do not configure these tools to take advantage of these Information Governance automation capabilities.

Manage schedules and automatically publish updates

Publish department and function-specific views of a schedule

Enable online retention schedule searching

Drag and drop document inheritance for retention, data security, and access control

Enable fully compliant automatic disposition

Automatically propagate and enforce changes to retention schedule changes

Figure 5. The Microsoft 365 suite of products has many native Information Governance capabilities. Source for list of capabilities: Contoural, Inc.

V. Automating Your Records Retention Schedule Management

The first stop for the records automation train is automating the publishing and access of the records retention schedule itself. The purpose of a policy is to communicate requirements and decisions. The easier it is for employees to get access to relevant information in your policy and schedule, the more effective they will be.

A. Moving Your Schedule Online and Making It Searchable

Traditional records programs create a schedule and publish it in either paper or PDF format. Records managers themselves may enjoy having a single consolidated view of records requirement in a single document; however this appreciation typically is not shared by employees who must manually search through these long schedules to find relevant records. If the process is too cumbersome, even well-intentioned employees will quickly abandon looking up information in the schedule.
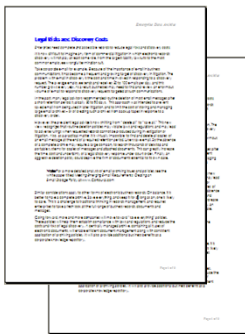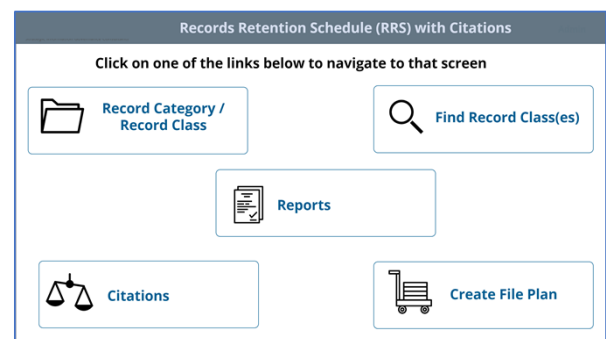
Figure 6. The traditional approach of distributing an entire schedule to employees and expecting them to manually search it to find records types is giving way to creating online and searchable schedules. The example above utilizes native Microsoft 365. Source: Contoural, Inc.

A smarter approach is to publish the schedule online using the native capabilities of systems already in house, making it web accessible and searchable. Employees can quickly login, and search for a record type. This is especially useful if the schedule contains sample record types, as the employee can then search for the relevant sample record to identify the record category. Publishing online also ensures that employees are always accessing the latest and most current schedule.

B. Automatically Publishing Department or Role-specific Views

Publishing a schedule online also provides the flexibility to publish department- and function-specific views of the schedule. These views contain records types that are relevant to a specific department, excluding record types that do not apply to the given function. Instead of having to look through an entire schedule, these narrower views allow employees to easily see in a single page or two their most relevant record types. All of this typically can be accomplished with technology that companies already have in-house.
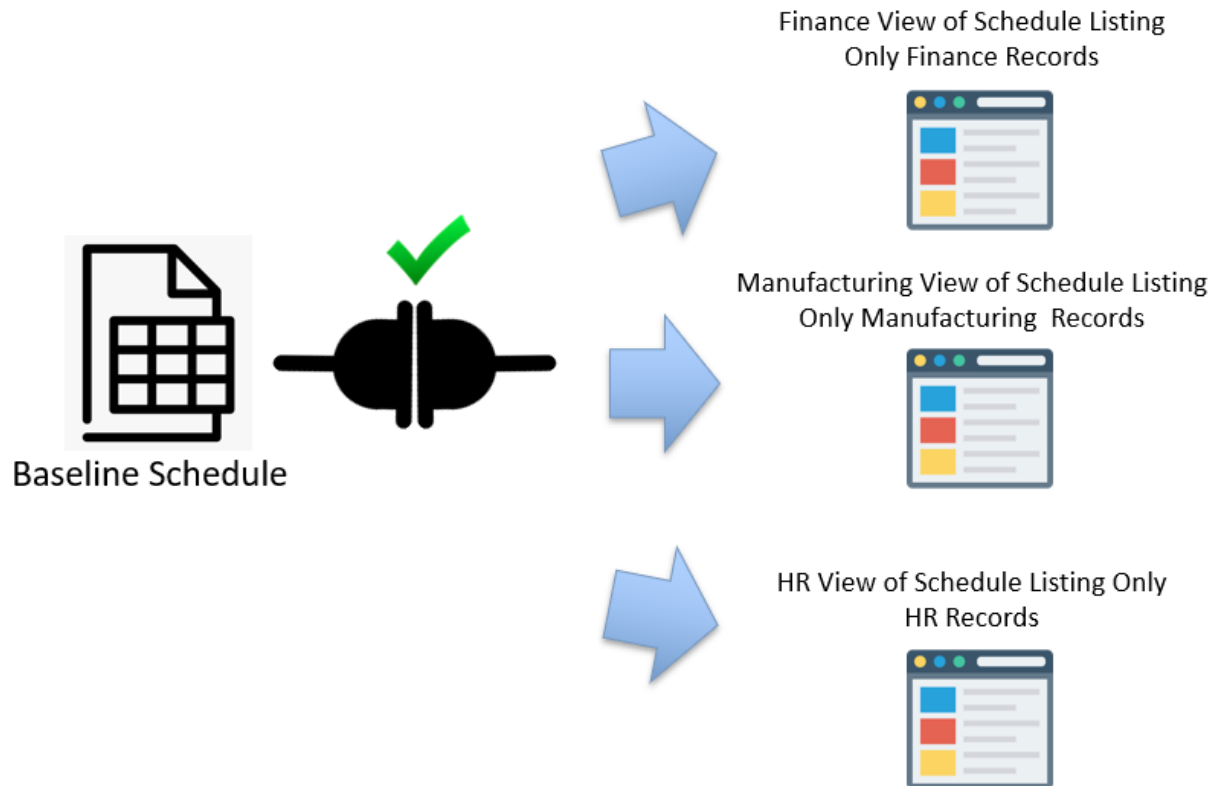
Figure 7. Provide each department with an excerpt of the schedule only containing records relevant to their function.

It should be noted that creating a department- or function-specific view requires both a well-designed schedule as well as expertise to decide how to present the correct information for any given department. These views are very organization-dependent and need to be customized for each company.

VI. Automating Records Classification

Making access to the schedule or a particular set of records within the schedule can be automated. Many companies provide automation at a more basic level through automated tagging of records based on where they are stored.

A. How "Drag and Drop" Auto Tagging Works

Most modern content management systems such as Microsoft 365, OpenText and others provide the ability to automatically apply metadata tagging (also referred to as labeling) based on where a record is stored. In other words, these systems allow a type of "drag and drop" tagging: Under this method, when employees drag and drop a file or email into a folder or specific location, the system automatically tags it. The system can automatically tag and track the document for multiple types of governance controls, including records retention requirements, data security classification, access controls and even legal hold capabilities. These retention periods, security levels and other policy attributes are pre-configured into a given managed folder. When the user places a document into the folder the content management system then automatically tags and applies these controls to the file. No action is required on the part of the user other than storing the document into the right folder; the system does the rest.
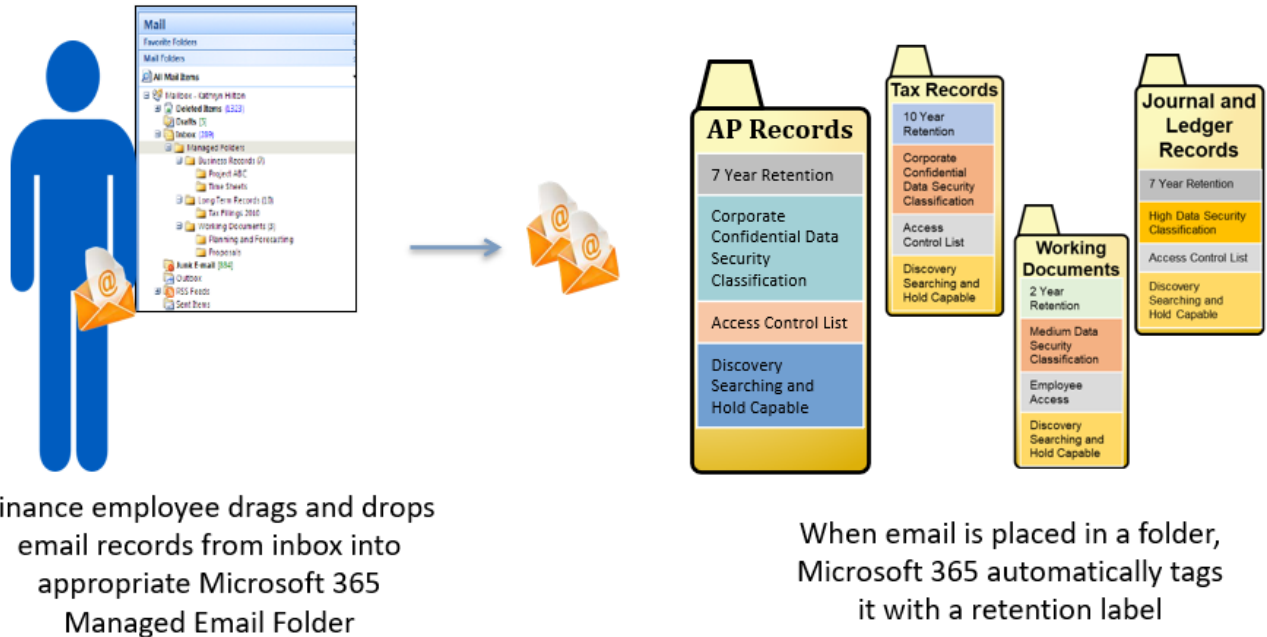
Figure 8. Microsoft 365 (described in this figure) and other content management systems have auto-tagging capabilities for automatically apply retention, data security classification, access controls and eDiscovery to emails, files and other documents stored within the system's folders. Source: Contoural, Inc.

B. Implementing Drag and Drop

This "drag and drop" classification strategy requires more upfront work. The Information Governance team needs to configure the managed folders or other repositories with the records retention, data security and access rules. Ideally, a complete Information Governance framework – retention, security, and access– should be configured. Translating the records retention schedule, data security classification and access control policies into specific system configurations can be tricky, and requires collaboration between the records, security, and IT groups.

While the backend configurations can be complicated, the user view and experience needs to be kept simple and intuitive. Different employees will have different folders to store their information, and collectively across the repository there may be many different folders. Any given employee should only see four or fewer folders. Recent innovations in these tools make it easier to consistently apply these rules while keeping it simple for employees.

Despite several Information Governance innovations, many companies have Microsoft 365 or other types of these repositories, but do not utilize them to their full capability. Why? It takes time and effort to configure and apply the rules correctly. Unfortunately, many of these systems are deployed on tight schedules, and the teams do not have the time or patience to configure them correctly. In these cases, these on-premise or cloud-based repositories resemble the same type of digital landfills as the file shares and desktops they replaced.

The upfront investment is worth it. Those companies that do take the time and effort to configure their systems for proper Information Governance may suddenly find classifying records, personal information, and other governed content much easier. Employees find the "drag and drop" approach easier. More information gets classified. And as discussed below, unneeded information gets compliantly deleted. Information no longer accumulates. Personal information is properly secured and managed. Employees are more productive. Syncing policies, processes with these technologies pays big information management benefits for many.

VII. Automating Records Disposition

It can be argued that saving files, emails and other types of electronic content is the easy part. The real test for an effective records program is how consistently and compliantly it can dispose of expired or unneeded, low-value content. This is an area where automation can offer some of its biggest benefits.

A. Letting Systems Automatically Dispose Records

Traditional manual records retention processes that require employees to selectively choose what to delete and when are ineffective, and worse, may create risk. First, when doing their own manual deletion, it is difficult for employees to be faithful and consistent to the records retention schedule. They tend delete what they consider the "bad stuff" – documents and other information they believe to be inculpatory and only save the "good stuff" — documents or files they believe will be helpful in the event of litigation or regulatory inquiry. Courts and regulators have been clear in stating good deletion should be a consistent, routine process based on policy.

The other challenge is simply getting employees to spend the time to delete the expired records. As discussed above, efforts to cajole or threaten them into manual process compliance quickly become ineffective. The root of this problem is not that they are bad employees, rather it is that the sheer volume of electronic information the average employee receives is overwhelming. Even spending 30 seconds per document translates to hours per week. Employees just won't do it. This inconsistency of employee deletion creates risk during eDiscovery or regulatory inquiry.

Figure 9. Repositories can be configured to automatically dispose documents when their retention period expires. This deletion can be suspended for legal holds. Source: Contoural, Inc.

For these reasons, many companies are enacting smart, compliant and automated deletion strategies. This approach removes the employee from the disposition process, and instead depends on leveraging technology to dispose of records when the retention period expires. To make automated disposition work, documents need to be classified per the "drag and drop" classification strategy discussed above when they are first received. Then the employees don't need to do anything. Microsoft 365 and other repositories will automatically dispose of documents once the expiration date has been reached, based on when it was entered into the system. The old information simply fades away.

Also keep in mind that there are some media and records types that are not managed on these "drag and drop" systems, including records in databases and of course paper. Nevertheless, emails and files represent the bulk of an organization's ROT and are usually the first target of litigators. Taming files and emails will go a long way in increasing compliance and lowering risk.

B. Disposing of Event-Based Records

Most records are time-based in that they need to be retained for a specific period that is known when the record is created. For example, most financial records need to be retained for seven years. There exists a smaller set of more difficult records to manage: event-based records. Event-based records are retained for a period after an event occurs. For instance, some employee records need to be retained seven years after an employee terminates. Of course, the employee termination is not known when the record is created.

Event-based records are harder to manage and compliantly dispose of. One approach has been to delete these only after the longest possible event occurs (i.e. after 30 years for employee records). This typically leads to the over retention of most records. A better approach is to develop an event-based trigger mechanism. Furthering the employee record example, as part of an employee's termination process, their records would be identified and the initial, post-event retention clock started. This entails developing the right business process triggers. Note that these event-based records are not easy. On the other hand, classifying a record as an event-based record and storing it in the appropriate repository makes creating these triggers much easier.

The other lesson here is that some type of records content is easier to manage than others. Files and emails can be managed easier than paper, which can be managed easier than database data. It is unlikely that content across all media can be managed in one single pass. Start with the easier media, then move onto the next and then work on remediating the last, harder pile. Even if you fall short on the last 20%, soon you will realize that the first 80% you did tackle greatly reduces risk, improves compliance, and cuts costs. Don't let your inability to address everything prevent you from addressing most things. In other words, do not let perfect be the enemy of good.

C. Automating Legal Hold to Suspend Auto Deletion

Fear of spoliation – fear of deleting information that an organization has a duty to preserve – inhibits employees and entire companies from disposing of expired records or unneeded content. Fortunately, the same "drag and drop" classification strategies discussed above can also greatly limit the risk of spoliation. These repositories enable holds to be placed across emails, files, and other documents. Even if a user deletes a document, the system still retains it until the hold is released or the retention period expires.

While these systems provide strong legal hold capabilities, two things need to occur. First, documents need to reside in the repositories. If all your information lives in file shares and desktops, having Microsoft 365 will not help you. Second, as discussed above, the legal hold process needs to be integrated with these systems.

D. Auditing and Remediating Your Records Processes

Regularly examining user and system conformance and compliance with records retention policies is important not only for ensuring that the approach is working; it also provides program defensibility in the event the adequacy of the company's compliance is challenged. Results of ongoing audits drive regular re-examination and refresh of policies, processes, and procedures. Typical records program audit areas include:

- Records training
- Records compliance across various groups
- Proper classification of record types, ensuring correct retention period
- Defensible disposition processes
- Legal hold implementation

Any weaknesses identified during an audit should be remediated. Likewise, audits should be an ongoing process to ensure continued compliance.

E. Trust Your Processes

Perhaps the biggest barrier to automating records deletion processes is fear. Fear that employees will not put all the information in the right place, and that some of it will be misclassified or retention will not be properly applied. Fear that records under legal hold will be deleted. Fear that records will be deleted before their expiration date.

The good news is courts and regulators do not expect perfection. Rather they expect reasonable, good-faith processes. Companies that develop good policies, implement good classification and disposition processes should then test and audit these practices. In doing so, they can relax. Defensibility comes from following your processes, checking them, and updating them.

VIII.Using Automation to Prevent Employees from Document Hoarding

The discussion so far has focused on classifying, managing, and deleting records. Of equal or greater concern to many companies is the ongoing accumulation of non-records. These include low business value information, duplicate copies of information and other digital junk that accumulates. Some employees have a *de facto* policy of saving everything forever. Automation can be employed to combat these document hoarders through a somewhat counter intuitive approach.

A. Creating a Working Document Strategy

Countering employee hoarding requires a different approach. Instead of trying to discourage employees from saving unneeded information, encourage them to save this information – but in the right place.

Within your Microsoft 365 or other content management system, provide a "working documents" folder. A working documents folder is an employee's personal file area that permits short-to-medium term retention. Allow employees to save whatever they want in these folders for whatever reason. Because they have been provided with a viable place to save any type of information in the working documents folder, prohibit them from saving unneeded information on desktops, file shares and other unmanaged and uncontrolled places. Explain to employees you are not stopping them from saving what they need, rather only asking they save it in the right place.

A working documents folder does not, however, enable employees to retain their files and emails forever. Set the retention for these folders anywhere from one to two years. Then let the system dispose the information when it expires. The key is that while employees can save whatever content they want, working document folders exist in a controlled and secure environment, with disposition automatically enforced. Microsoft 365 and other repositories are terrific at saving information. They are even better at deleting it.

In one sense, working documents folders provide a safe and approved version of the "underground archiving" behavior discussed above. There are no restrictions on what can be saved. Likewise, there should be no reason employees would need to engage in actual underground archiving. They have been provided a place to store information.
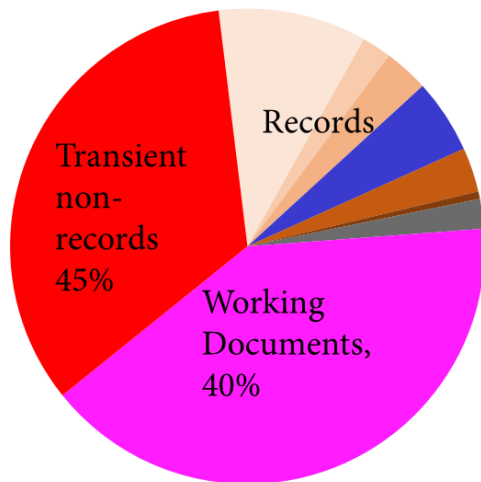
Working Document: Short-term transitory record employees need to do their jobs and be productive.

Examples: Projects correspondence, draft presentations, contract negotiations, yearly holiday schedules

Transient Non-records: Documents that do not need to be retained as records that have low or no business value.

Figure 10. Allow employees unlimited ability to save working documents in a searchable, centrally managed controlled repository, typically a managed folder. Auto-delete these working documents after established period of two to three years.

B. Sweep Email Boxes After 90 Days

Once records management and working documents folders are configured, employees should be trained to drag and drop emails from their inbox into one of these folders. Everything that needs to be retained, or an employee wants to save should be moved to these folders. It can be assumed that any email left in an employee's email inbox for more than 90 days is truly junk – it is neither a record nor does it have any transitory business value (otherwise it would have been saved in the working documents folder). It is now safe to automatically delete email older than 90 days from the inbox.
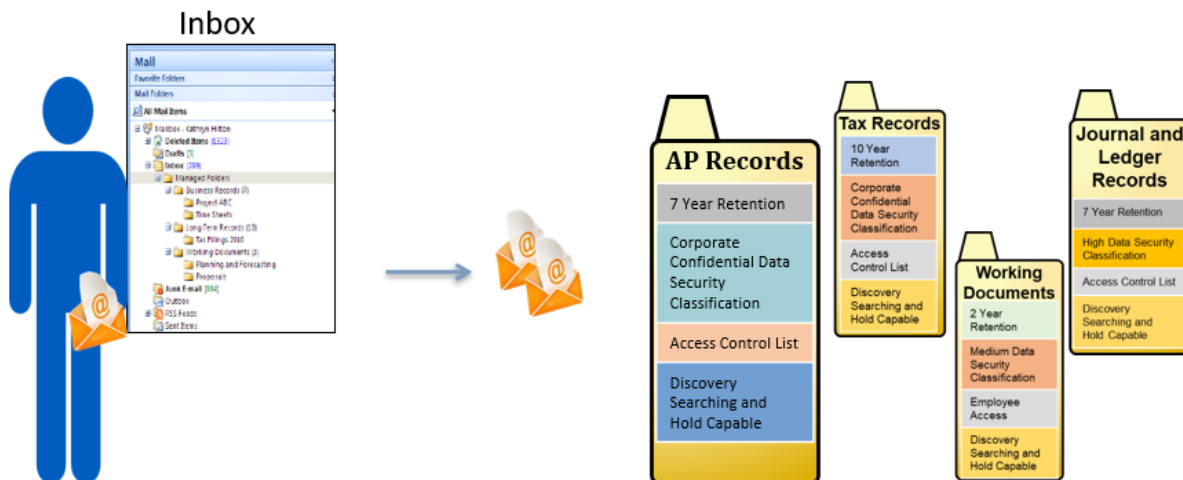
Finance employee drags and drops email records from inbox into appropriate Microsoft 365 Managed Email Folder

When email is placed in a folder, Microsoft 365 automatically tags it with a retention label

C. File Share Scanning Tools

Within the past few years newer file share scanning and analytic tools have emerged on the market. These tools use a variety of pattern matching and other analytic techniques to identify the content in files and emails and (hopefully) classify the type of document. Today these tools have three main use cases. First, they can identify personally identifiable information (PII) such as addresses, social security numbers and a subset of other types of personal information. Second, they can be beneficial in migrating content from say files shares and desktops into Microsoft 365 systems; storing documents in the right location based on content (as discussed above, this process requires a significant amount of training). Finally, they have successfully been used to identify the low-level ROT in file systems such as duplications, older versions and other easy-to-identify low value content.

The challenge with these tools is that they are reactive. They can remediate file shares after they fill up with the unneeded content or personal information. However, they don't stop the unnecessary saving and filing of documents. In other words, they don't identify how the personal information made its way into the file share to begin with. A file scanning strategy will have to continuously scan.

D. Diligently Train and Manage (Against) Paper Retention

The final challenge of over retention is in paper documents. Employees print and save a myriad of electronic information, much of which makes it into longer term and expensive off-site storage facilities. Much of this information was sourced as electronic information, which should already be retained.

Most over-retention of paper tends to be a training issue. Many employees believe that only a paper copy of a record is an "official" copy. Today, very few records need to be saved in paper with a hand-written signature. Most records can be saved electronically, and the handful of exceptions should be noted in an organization's records retention schedule. Finally, sometimes employees will hoard paper copies of electronic documents for fear that the electronic version will be taken away or that they will not be able to find it when they need it. Implementation and training of the working document strategy discussed above should decrease employees' need to make a "just in case" paper copy of a document.

IX. Conclusion: The Real, Hidden Win of Automation

Many organizations update their records programs and add automation to drive better compliance, reduce costs and reduce risks. Somewhere along their journey they find that these strategies not only drive compliance, but also make useful information easier to access and collaborate. Records programs are valued less for their compliance capabilities, but rather for increasing productivity. Employees spend less time searching through redundant, obsolete, and trivial information, and instead find relevant, higher value information more easily. They actually like using records management systems because it makes them more productive. Records automation makes life easier not only for Information Governance professionals – perhaps the biggest win is for employees.

X. About the Author

Mark Diamond is an industry thought leader in information governance, encompassing records and information management, litigation readiness, control of privacy and other sensitive information, defensible disposition, and employee collaboration and productivity. Mark is a frequent industry speaker, presenting at numerous Legal and IT industry conferences. Additionally, Mark delivers more than 50 onsite Information Governance seminars to internal corporate audiences each year.

Mark is the founder, President & CEO of Contoural, Inc. Previously, Mark was co-founder of Veritas' (OpenVision) Professional Services group; founder and General Manager, Worldwide Professional Services for Legato Systems; and Vice President of Worldwide Professional Services at RightWorks. He has also worked as a management consultant. He also served as Chair of the Storage Networking Industry Association's customer advisory board on data security. He sits on the board of advisors for high technology companies.

He has a bachelor's degree in Computer Science from the University of California San Diego. Mark is former President of the UC San Diego Alumni Association, and served as a Trustee of the university's foundation.

Mark welcomes any questions and comments regarding this Guide. He can be reached at mdiamond@contoural.com and for more information, on Contoural's site at

www.contoural.com.

XI. About Contoural

Contoural is the largest independent provider of privacy, Information Governance consulting services focused on California Consumer Privacy Act (CCPA), General Data Protection Regulation (GDPR), Records and Information Management, litigation and regulatory inquiry readiness and control of privacy and other sensitive information. Contoural does not sell any products or take referral fees, store any documents or provide any lawsuit-specific "reactive" e-discovery services, serving as a trusted advisor to its clients providing unbiased advice. Contoural has more than 30% of the Fortune 500 as clients, across all industries, as well as federal agencies and local governments. Contoural offers a range of privacy and Information Governance services:

- Records Retention Schedules

- Data Privacy Maturity Assessment

- Personal Data Inventory

- Data Mapping

- Privacy Policies and Procedures

- Privacy and Security Enhancements

- Technology Requirements for Privacy and Security Controls

- Taxonomy & File Plan

- Implement Privacy and Security Controls

- Privacy Communications and Training

- Legacy Data Remediation

XII. Additional Resources

A. ACC Maturity Model Resources

[ACC U.S. States Privacy Capability Maturity Model](#), ACC Information Governance Network

[ACC Records Management Maturity Model](#), Legal Operations Network

B. ACC Guides

"Information Governance Primer for In-house Counsel," (2016), *available at* https://www.acc.com/resource-library/information-governance-primer-house-counsel

"Creating a Modern, Compliant, and Easier-to-Execute Records Retention Schedule," (2017), *available at* https://www.acc.com/resource-library/creating-modern-compliant-and-easier-execute-records-retention-schedules

"Executing Your Records Retention Policy and Schedule," (2018), *available at* https://www.acc.com/resource-library/executing-your-records-retention-policy-and-schedule

"Operationalizing the California Consumer Privacy Act," (2019), *available at* https://www.acc.com/resource-library/operationalizing-california-consumer-privacy-act-united-states

C. ACC Docket Articles

"Everybody's Job, Nobody's Job: The Best Way to Create an Information Governance Program Without Going Crazy," Patrick Chavez and Mark Diamond, *ACC Docket* (April 2019) *available at* https://www.accdocket.com/articles/resource.cfm?show=1500001

"Upgrading Your Traditional, Paper-centric Records Program to Be More Modern, Compliant, and Useful," Andrea Meyer and Mark Diamond, *ACC Docket* (December 2018) *available at* https://www.acc.com/resource-library/upgrading-your-traditional-paper-centric-records-program-be-more-modern-compliant

"Building a Business Case for Information Governance," Annie Drew and Mark Diamond, *ACC Docket* 32, no. 8 (Oct. 2014): 26-40, *available at* https://www.acc.com/resource-library/building-business-case-information-governance-program-2016

"Privacy Trends: The California Privacy Act is a Harbinger of New Regulations," ACC Docket March 2019, *available at* https://www.accdocket.com/articles/resource.cfm?show=1497947

D. ACC Legal Quick Hits

"How to Operationalize Compliance for CCPA," *Legal Quick Hit*, (2019), *available at* https://www.acc.com/education-events/2019/how-operationalize-compliance-california-consumer-privacy-act

"Personal Data Inventory and Data Mapping Strategies," *Legal Quick Hit,* (2019), *available at* https://acc.inreachce.com/Details/Information/69ebaee4-c3bd-4447-81ff-d1e092461af1

"Preventing Employees From Hoarding Documents," *Legal Quick Hit,* (2018), *available at* https://acc.inreachce.com/Details/Information/FAA4D598-2313-4693-B408-2E5C09CB94C3

E. ACC – Webcasts

"Creating a Records Retention Schedule That Does Not Create Problems (And Actually Solves Them)," *Webcast* (2020), *available at* https://acc.inreachce.com/Details/Information/ec5b0127-7915-4bdc-a874-dc202568b0b0

"IG 101: Information Governance for In-House Counsel Parts 1 and 2," *Webcast* (2019), *available at* https://acc.inreachce.com/Details/Information/3a9b3a20-d3dd-42fd-bb70-863dd70542d7

"Legal Operations Maturity Model Series - Information Governance & Records Management," *Webcast* (2019), *available at* https://acc.inreachce.com/Details/Information/a0edf21b-3014-4676-b70b-cd5a1398637b

"Information Governance: Getting a Program Started," *Webcast,* (2017), *available at* https://acc.inreachce.com/Details/Information/88a31407-7ff2-42df-8d59-6da965f96de1

F. ACC – Information Governance Network Resources

"Understanding the California Consumer Privacy Act (CCPA)," *Quick Overview*, (2019), *available at:* https://www.acc.com/resource-library/quick-overview-understanding-california-consumer-privacy-act-ccpa

"Information Governance – Glossary of Terms" (2019), *available at* https://www.acc.com/resource-library/information-governance-glossary-terms

"Employee Behavior Change Management Programs for Information Governance," *Quick Overview*, (2017), *available at* https://www.acc.com/resource-library/employee-behavior-change-management-programs-information-governance

"Creating a Data Classification Standard," (2017), *available at* https://www.acc.com/resource-library/creating-data-classification-standard

"Data Map Design Strategies," (2017), *available at* https://www.acc.com/resource-library/data-map-design-strategies

"Data Map Use Cases," Sample Forms, Policies, & Contracts, (2017), available at https://www.acc.com/resource-library/data-map-use-cases

G. Contoural Whitepapers

"Creating a California Consumer Privacy Act Action Plan," *White Paper,* (2019), *available upon request at* https://www.contoural.com/whitepaper_summary.php?id=43 on Contoural's website www.contoural.com

"Reducing Your Offsite Paper Storage Risk and Cost," *White Paper,* (2018), *available upon request at* https://www.contoural.com/whitepaper_summary.php?id=40 on Contoural's website www.contoural.com

 "Defensible Disposition: Real-world Strategies for Actually Pushing the Delete Button" *White Paper,* (2014), *available upon request at* http://www.contoural.com/whitepaper_summary.php?id=31 on Contoural's website www.contoural.com

"Stop Hoarding Electronic Documents," *White Paper,* (2012), *available upon request at* http://www.contoural.com/whitepaper_summary.php?id=32 on Contoural's website www.contoural.com