WHITE PAPER

# Building a Modern Information Governance Strategy

## New Information Management Landscape Requires a New Approach

**Abstract**

Information management is getting harder. Organizations face increasing data volumes, more stringent legal and regulatory recordkeeping requirements, stricter privacy rules, increasing threats of breaches and decreasing employee productivity. Companies are also finding that their older, legacy archive strategies are increasingly ineffective in this new environment. This is driving organizations to rethink their approach, developing more modern Information Governance strategies centered around electronic information. This white paper discusses these information management challenges and details how they can be addressed through a modern Information Governance strategy.

Sponsored by:

mimecast®

contoural

READY. COMPLIANT. IN CONTROL.

# The Information Management Landscape is Changing

**New and stricter legal and regulatory requirements coupled with ongoing accumulation of electronic information are creating new risks and challenges for companies. These changes are occurring globally. Traditional archiving approaches fall short of meeting these new requirements, and this is driving many companies to re-examine how they manage information.**

## Increasing Compliance Requirements

While more information is being retained, the legal and regulatory requirements are getting stricter. According to ARMA, the average global corporation faces more than 30,000 legal and regulatory recordkeeping requirements. The past decade has seen a spate of new requirements at the federal, state, and industry-specific levels. These include, for example, regulations such as Dodd Frank, as well as updates to existing retention requirements from FINRA in the US or IIROC in Canada or FCA in the UK. Equally difficult are organizations with a global footprint facing regulations from multiple countries.

## eDiscovery is Getting Harder

The ongoing accumulation of both paper and electronic information creates very acute challenges when organizations face discovery in litigation or from regulatory inquiry. First, the sheer volume and expanse of electronic information increases the risks of being non-responsive to a discovery request. Not knowing what a company has often forces them to look through everything. Second, the increasing volume and lack of controls significantly increase discovery costs and impact litigation strategies. It should be noted that under newer discovery rules in the U.S. and Canada, organizations that can identify what they have early in the process may be able to produce less information. Yet this strategy is often difficult to implement in a "save everything, everywhere" type of information management environment.

## New Privacy Requirements

Global privacy rules are changing the information landscape. Historically many organizations have approached electronic records retention with a de facto "save everything, forever" approach thinking that in doing so they would at least be meeting regulatory retention minimums. New global privacy rules, however, add a completely different twist: whereas before companies could save everything forever, new global privacy rules specifically require organizations to dispose of unneeded privacy information. This privacy information exists in databases, files, email and paper documents. The European Union's General Data Protection Regulation requires organizations to keep personal data only so long as necessary to fulfill the original basis for collecting and processing it — and no longer. Hence a "save everything, forever" strategy will drive noncompliance.

Europe's privacy laws are serving as a model for other privacy legislation, including the California Consumer Privacy Act as well as rules being adopted by other countries. Similar to the European rules, California's Consumer Privacy Act gives consumers the right to know what personal information has been collected about them and with whom it has been shared. Likewise, California consumers can request the deletion of their personal information. Significant penalties exist for non-compliance. These privacy rules are likely to significantly change how organizations collect and manage information.

### Is Email Really a Record?

Traditionally many organizations have treated email as a transitory document that does not contain any records. This approach is incorrect and non-compliant. Records are determined not by media, but rather by content. Literally all organizations have some records in email and some exist exclusively in email. This has been affirmed by both courts and regulators, and companies that have not managed records in email have been subject to fines and regulatory actions. These email-based records have been described by some as "inventory resistant" because, unlike paper records where compliance can be measured by counting the number of boxes going into a warehouse, most electronic records accumulate on employees' computer hard drives and are not as easily inspected. Email records are real and must be managed appropriately.

CASE STUDY

### Financial Services Firms Face eDiscovery Challenges

Shortly after the financial crisis in 2007 many US financial services firms faced investigations both from Federal and State regulators. These broad inquiries required these firms to preserve relevant documents including significant quantities of emails. Many investigations dragged on in for years, and these firms continued to preserve older emails as well as save new emails.

When these investigations were finally adjudicated, some firms had literally hundreds of millions of emails in archives, and they faced a dilemma: the majority of the emails in the archives were either expired records or non-records that should be deleted per their retention policies, but the companies had no way to classify which emails were active records that still needed to be retained and which emails were expires records and non-records to be deleted. Unable to classify their records properly, this forced many firms to continue retaining massive quantities of email, significantly driving up discovery costs for any new investigations or litigation.

Many are still stuck with huge quantities of emails in legacy archiving systems.

## Need to Protect Sensitive Information from Breaches

Many organizations know their information landscape contains significant intellectual property, trade secrets and other types of sensitive information. They mistakenly believe that as this information is stored on corporate file shares or content management systems they are protected. Nevertheless, even in tightly controlled environments, sensitive information often leaks from secure to unsecure areas. Employees, contractors and other authorized individuals often store confidential or sensitive data on corporate file shares, in email, or on portable devices (such as unencrypted laptops and USB and flash drives). Once in this unsecure location, the data may simply be forgotten. Since unsecured repositories have an inherent lack of access control, it still represents a potential risk of a data breach or data leak. Couple the ever-increasing volumes of data that organizations are accumulating with the growing number of potentially unsecured places that data may reside, the risk of a breach or leak is much greater. Exacerbating the problem is the fact that employees are often unaware that they are prohibited from storing data in a particular location, or worse, the company may not have a policy prohibiting this type of behavior or have any specific training on how to deal with particular types of information.

*"I spent my first three months on the job searching through my predecessors' email. I had to look for everything from offer letters to employee reviews, spending hours every week. What a nightmare."*

*— Vice President of Human Resources for a mid-sized high technology company*

## Impacting Employee Productivity

While poorly managed information creates a number of legal, regulatory and security challenges, it can also significantly impact and decrease employee productivity. Employees who have adopted a "save everything just in case I need it" approach for email and files (documents) soon find it difficult to find their own information among the clutter. Gartner Research, Inc estimates that the average employee wastes more than 3.5 hours per week locating emails or the correct version of files. This problem is compounded when departments face employee turnover. Today, many employees store key information in their own individual silos on file shares or within their own personal email stores. When there is employee turnover this information is effectively lost and the employee's successor is often forced to reinvent the wheel.

## Older Approaches Do Not Work

Many of the information management processes in place today are based on either a paper-centric paradigm of dumping email and files in an archive or on an outdated, vaulted solution where information goes to die. This "dumping" strategy creates risks and increases costs:

**Not managing email and electronic information as a record:** Many programs do not recognize that records exist in email and other electronic media. These records are not properly classified or managed. Retrieving these records in a timely manner can be difficult, and often no effort is made to dispose of them once their unacknowledged retention period has expired.

**Over-reliance on detailed, manual processes:** Programs that do recognize requirements of managing electronic information often make employees walk through detailed and time-intensive recordkeeping processes to comply. Employees need to search through overly-detailed records retention policies, classify and retain these records through a series of time-consuming steps.

**No defensible disposition processes:** Unmanaged electronic information accumulates. New information and documents are continually created, received and saved, but little effort is made to dispose of older, unneeded information. Every year the storage of this unneeded information grows, driving up risks and costs.

**Need for greater employee productivity:** These old-fashioned approaches decrease employee productivity. Current business information is lost among the clutter of unneeded information. Every employee has his or her own "silo" of information making it difficult to share or collaborate. Poor information management makes organizations less agile and responsive.

Continuing with these old-fashioned approaches increases costs and risk, drives non-compliance and lowers employee productivity. A more modern approach is needed.

# Need for a Modern Information Management Strategy

Many organizations are rethinking their information management programs. They are creating modern and easier-to-execute policies, developing comprehensive processes and deploying better technology, all of which not only drives compliance but also increases employee productivity.

## Start with a Modern, Compliant and Easier-to-Execute Records Retention Schedule

The shift to electronic as the primary communication medium for information has changed how organizations create, receive, share and collaborate information. It therefore makes sense that the policies and schedules to drive the identification, classification, retention, retrieval and disposition of this information should also change.

A key first step to gaining control over these problems is developing a modern, compliant and easier-to-execute records retention policy and schedule. At its core, a policy and schedule not only define legal and regulatory recordkeeping requirements, but also build

a consensus across key stakeholders, business units and employees on what should be saved and for how long, as well as what can and should be deleted. Modern policies and schedules include records across all media, reflect current legal and regulatory requirements and account for the business value of information. Additionally, they integrate with other compliance regimes including privacy and discovery, are easier for employees to understand and follow and are maintainable.

## Effective Data Security Classification

A cornerstone of any information management program is identifying, classifying, securing and disposing of privacy, intellectual property, trade secrets and other types of sensitive information. Modern programs build data security classification directly into their information management programs. This includes developing a detailed analysis of the flow of private, sensitive, personally identifiable information (PII) and evaluating the effectiveness of existing controls with respect to applicable internal policies and external regulations. Equally important, they are moving information for unmanaged and unsecure repositories to managed, controlled and secured repositories. This focus of including privacy and security into the information management program minimizes the risk of data breaches and any misuses of sensitive or critical information, which in turn improves user compliance through steam-lined and easy-to-understand categorizations.

> *"There is a growing campaign by the plaintiffs' bar to target data privacy and security in the hopes of striking it rich in a new goldmine on the level of the asbestos litigation of the 1970s, 1980s, and 1990s."*
>
> *— Engineered Liability: The Plaintiffs' Bar's Campaign to Expand Data Privacy and Security Litigation*

Protecting sensitive information from breaches requires two important elements. First, files and emails and other documents containing sensitive information should be stored and managed in appropriately secured repositories. This often means moving them from desktops and files shares to more secure archives. Second, organizations need to implement controls within the archive to defensible destroy sensitive information when it is no longer needed. This can include when records have reached their expiration data, or the information no longer has business value.

## Proactive Litigation Readiness

Many organizations are moving from reactive eDiscovery to proactive litigation readiness programs. To do so, they must take a step back, get away from their lawsuit-specific activities and look at what can be done to improve their litigation readiness profile. These programs include updating legal hold policies to incorporate eDiscovery response processes as well as developing processes to map electronic information. This approach includes creating repeatable, defensible processes for how the organization manages and responds to requests for information regardless of location or format. All of these elements of the legal hold process should 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. Equally important, these programs incorporate effective technology. By developing an information management program inclusive of a legal hold policy that includes eDiscovery protocols, organizations will be better prepared to address lawsuits as well as any legal or regulatory changes that may occur.

## Driving Employee Productivity

Perhaps the biggest "win" from a modern program comes from better employee productivity and enhanced collaboration. Modern processes and technologies allow employees to 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.

Some "wins" for employees under these updated records programs include:

- Have full search capability
- Keep documents organized the way employees work
- Easier to share valuable content
- Ability to always locate the most current version
- Not worry about what data needs to be kept with automated disposition
- Use mobile device for certain types of information
- Valuable information is available and not lost in the clutter
- Have no worries if laptop crashes or mobile device is lost or stolen

While modern information management programs are often started in response to privacy or other new compliance requirements, companies soon realize the biggest driver of these programs is the boost to employee productivity.

## Enabling Both Targeted and Ongoing Defensible Disposition

It can be costly to hold on to information that is obsolete, expired, and not needed for legal, regulatory or business reasons. More important, new privacy regimes require the disposition of privacy information. Disposition is being divided into two separate processes. First, organizations are deploying targeted disposition to, for example, delete personal information from a GDPR "Right to Erasure" request by a European citizen. Once these requests are received, organizations first need to identify any privacy information across all media, including files and email. Save any recordkeeping requirements, this information then needs to be selected and deleted.

Second, modern strategies have routine, ongoing processes to delete expired records along with unneeded or low business value information. This is again for email, files, paper and other types of media. Likewise, these disposition processes need to respect ongoing records retention periods, as well as legal hold processes. Disposition should be targeted both at active data including email in servers and files on file shares, and also at inactive data on backup tapes.

# Final Word: Putting the Pieces Together in an Information Governance Strategy

Modern strategies engage a number of drivers including legal and regulatory recordkeeping requirements, stricter privacy rules, increasing threat of breaches and decreasing employee productivity and disposition. A modern strategy not only incorporates all of these drivers, but increasingly transforms stand-alone records, privacy and discovery programs into an integrated Information Governance program. Companies are realizing that a single common workstream under an Information Governance program can provide benefits in a number of areas. In the end, these modern approaches not only increase compliance, but markedly reduce costs, reduce risks and drive productivity.

# About Mimecast

Mimecast (NASDAQ: MIME) makes business email and data safer for thousands of customers and their millions of employees worldwide. Founded in 2003, the company's next-generation cloud-based security, archiving and continuity services protect email and deliver comprehensive risk management.

Mimecast Cloud Archive is a multi-purpose, cloud-based solution that serves the needs of legal, compliance and IT leaders. With capabilities to manage retention, e-discovery, compliance and supervision, Mimecast Cloud Archive helps reduce cost, complexity and risk while bringing greater insights and decision-making power to the people who need it.

# Additional Materials Available

Please visit www.contoural.com for the following materials.

## Complimentary Webinars

- Records Retention Policy and Schedule Development
- Records Retention Policy and Schedule Refresh
- Records Schedule Citation Development and Legal Review
- Records Management and Information Governance Maturity Assessments, and Strategic Roadmap Development
- Enterprise Behavior Change Management
- Legal Hold and Discovery
- Technology Requirements and Adoption
- Legacy Paper and Data Disposition
- Email and Unstructured Data Placement
- Records Management and Information Governance Organizational Development and Governance

## White Papers

- Stop Hoarding Electronic Documents
- Metrics Based Information Governance
- Email Classification Strategies That Work
- Is It Time For Auto-Classification? Parts 1 and 2
- Ten Elements of Electronic Records Retention
- Seven Essential Storage Strategies
- Six Steps to Controlling eDiscovery for Email
- Ensuring Compliance and Reducing Risk
- Archiving Approaches
- What Do We Do With Legacy Data?

# About Contoural

Contoural is the largest independent provider of information governance consulting services focused on Records and Information Management (RIM), litigation and regulatory inquiry readiness and control of privacy and other sensitive information. We do 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 our clients providing unbiased advice. We have 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 record management and information governance services:

- Records retention policy and schedule development
- Records retention policy and schedule refresh
- Records schedule citation development and legal review
- Records management and information governance maturity assessments, and strategic roadmap development
- Enterprise behavior change management
- Legal hold and discovery
- Technology requirements and adoption
- Legacy paper and data disposition
- Email and unstructured data placement
- Records management and information governance organizational development and governance



contoural

READY. COMPLIANT. IN CONTROL.

335 Main Street, Suite B, Los Altos, CA 94022

650.390.0800 | info@contoural.com | www.contoural.com