Technology
Consulting
Associates

Email Record Management

P.O Box 420076
Atlanta, GA 30342
Phone 877.842.1842
Fax 404.943.9081
www.tca-llc.com

The content of this Insight document should not be construed as specific professional advice or services for your business by Technology Consulting Associates, LLC.

Before making any decision that might affect your finances or business a qualified professional advisor should be consulted.

Emails must be managed as a business record to avoid undue risk associated with regulatory non-compliance and litigation. There are three (3) stakeholders involved in email record management:

1. *Business users*
2. *Legal, risk, and regulatory departments*
3. *IT departments*

and four (4) major functions:

1. *Create and Use*
2. *Retain and Archive*
3. *Store and Secure*
4. *Dispose*

Commercial Off-The-Shelf (COTS) products and services are available for email record management but they should be implemented in a methodical manner.

Insight Objectives 4
Audience 4
Email Record Management 5
Why Manage Email 5
Who Is Impacted........ 5
Stakeholder Requirements 6
Business Users........ 6
Legal, Risk, and Regulatory Departments 7
Legal and eDiscovery 7
Regulation, Compliance and Records Information Management 10
Information Technology (IT) 11
Processes........ 12
Create and Use 12
Retain and Archive 15
Email Retention Approaches........ 15
Retention Policy 18
Store and Secure 21
Discovery and Hold........ 22
Dispose........ 23
Implementing eMail Record Management 24
Email Record Management Planning 24
COTS........ 25
Methodical Development and Implementation........ 26
Insights 27
How TCA Can Help 28

Insight Objectives

This TCA *Insight* paper provides information relevant to business operations, compliance, and risk management.

Audience

The following individuals should find this *Insight* useful:

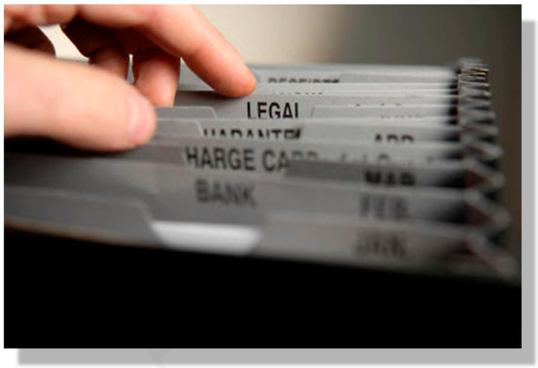
- Executive administrative management
- Legal executive and operational management
- Regulatory executive and operational management
- Information technology executive and operational management

Email Record Management

Why Manage Email

The International Organization for Standardization (ISO) defines a business record as "information created, received, and maintained as evidence and information by an organization or person, in pursuance of legal obligations or in the transaction of business". Put simply, a business record can be defined as "evidence of an event".

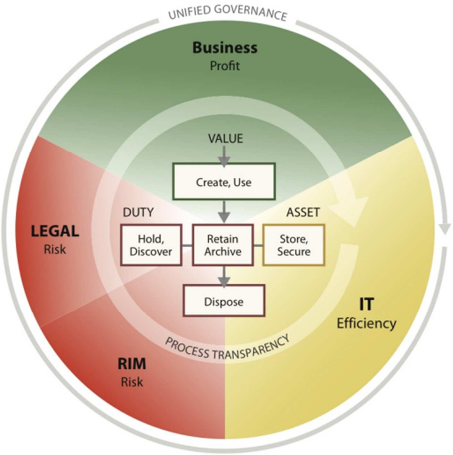
Emails sent or received because of a business policy, or duty to report or record the information contained in the email, are considered business records.[1] As potential business records emails need to be managed as an information asset of the company.



Failure to manage emails appropriately place an enterprise at risk from both regulatory non-compliance issues and litigation costs.

Who Is Impacted

The Information Management Reference Model (IMRM) produced by EDRM[2] provides a framework for illustrating who and what is involved in an email record management effort.



EDRM identifies three major stakeholders involved in the management of email:

1. Business users who need information located in email to operate the organization
2. Legal, risk, and regulatory departments who understand the organization's duty to preserve the information located in email beyond its immediate business value
3. IT departments who must implement the mechanics of email management

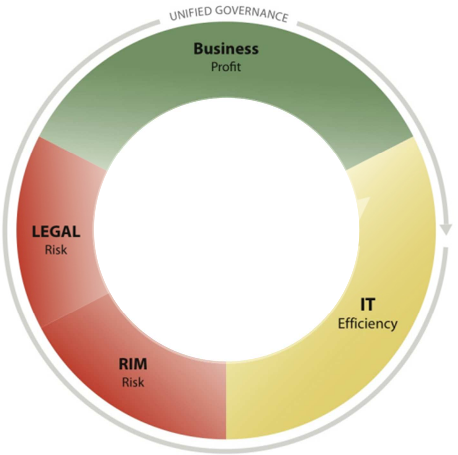
[1] Oil Spill by the Oil Rig "Deepwater Horizon" in the Gulf of Mexico, on April 20, 2010, MDL No. 2179, 2012 WL 85447 (E.D. La. Jan. 11, 2012) identifies five requirements that a party has to satisfy in order to show that an email is subject to the business records exception:

- *The email must have been sent or received at or near the time of the event(s) recorded in the email.*
- *The email must have been sent by someone with knowledge of the event(s) documented in the email.*
- *The email must have been sent or received in the course of a regular business activity, which requires a case-by-case analysis of whether the producing defendant had a policy or imposed a business duty on its employee to report or record the information within the email.*
- *It must be the producing defendant's regular practice to send or receive emails that record the type of event(s) documented in the email.*
- *A custodian or qualified witness must attest that these conditions have been fulfilled.*

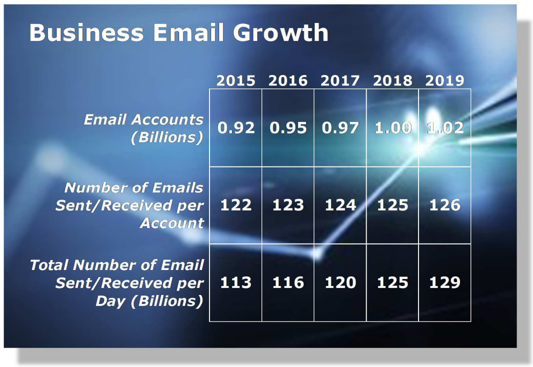
[2] Electronic Discovery Reference Model (EDRM) develops guidelines, sets standards and delivers resources to help e-discovery consumers and providers improve quality and reduce costs associated with e-discovery

Stakeholder Requirements

All three major stakeholders have unique email requirements. In order to understand an enterprise's Email Record Management needs and ensure that an appropriate solution is developed all three stakeholders must be engaged.



Business Users



Business Email Growth

	2015	2016	2017	2018	2019
Email Accounts (Billions)	0.92	0.95	0.97	1.00	1.02
Number of Emails Sent/Received per Account	122	123	124	125	126
Total Number of Email Sent/Received per Day (Billions)	113	116	120	125	129

Email has become a ubiquitous business tool. An estimated one billion business email accounts exist today, and the number is expected to continue to grow. A typical business email account receives and sends over one hundred and twenty-five (125) emails every day. This results in an estimated 1.25 billion business emails processed every day![3]

The uses of email are as varied as the companies, departments, functions, and people attached to the email accounts. Typical uses include:

- *Information Exchange* –a primary communication device between individuals, within small and large groups, and for general announcements.
- *Brainstorming and Problem Solving* –solicit ideas and potential solutions prior to actual face-to-face contact to increase the efficiency of actual meetings
- *Record Keeping* –maintain organized email archives for easy access to information that may be needed in the future
- *Group Work* - supports collaborative document production
- *Staying in Touch Professionally* - email "list-serve" functions are an increasingly common way to keep track of recent developments and current trends in a field. Interested people join a group and whenever any member sends an email message to the list, all members get the message.
- *Staying in Touch Socially* – in many cases email has replaced telephone calls and letters that used to keep family and friends in touch. Even though many businesses have policies against the use of corporate email for personal use, it is common practice.
- *Transmitting Documents* – In many cases email has replaced the fax as a primary method of transmitting documents within an organization and between organizations.

In addition to these uses, many companies set up special purpose email accounts to receive customer and vendor requests/complaints, employee suggestions/grievances, and even customer orders.

[3] *The Radicati Group, Inc. Email Statistics Report, 2015-2019*

Legal, Risk, and Regulatory Departments

Legal and eDiscovery

On December 1, 2006, several key changes to the Federal Rules of Civil Procedure (FRCP) involving electronic discovery became law. While most of the changes involve the way electronic information is handled during a litigation procedure, there were two major changes which affect virtually all companies doing business in the U.S.:

1. The term "data compilation" was replaced by the phrase "electronically stored information" (ESI), representing a broader term to include all digitally stored records *including emails*.
2. There was a fundamental shift from electronic data being included by exception only to now being excluded by exception only. This means that all discovery requests include email unless otherwise specified.

Subsequent decisions have shown that:

- The courts are not tolerant of organizations that have not implemented timely programs to accurately retrieve email
- Companies must prove that a policy for retention and litigation hold is enforced
- Penalties for failing to meet the FRCP deadlines can be high
- Limited staff and resources are not excuses for missing deadlines

As a result of these rule changes and court decisions, the majority of discovery orders in the U.S. today require email to be produced as part of the discovery process. In order to respond to these requests organizations follow a process that can be explained using the Electronic Discovery Reference Model (presented in more detail later in this document). Basically the legal department must:

1. Identify, preserve and collect what emails might be relevant
2. Process, review, and analyze those emails
3. Produce and present emails to relevant parties

Without appropriate processes and systems outside parties may have relevant emails that do not exist within the company!

Identifying, preserving, and collecting emails in response to a discovery order can be costly since unmanaged emails can exist in many places – backups, desktop and laptop PCs, mail server, file shares, etc. These steps typically require extensive interaction between legal and IT.

Processing, reviewing, analyzing and producing emails can take an extraordinary effort. Such eDiscovery efforts are estimated to represent 35% of the total cost of litigation[4]. Typically this work is outsourced to legal firms which charge $100s per hour, representing substantial cost to an enterprise.

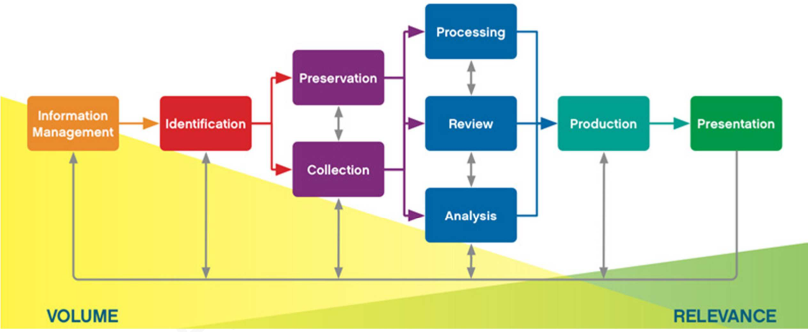
[4] *Pillsbury Winthrop Shaw Pittman LLP*

Examples of Inadequate Email Record Management

Complete Information	During the lengthy anti-trust case between Intel and AMD, Intel said that it set a firm, clear retention policy in place once it learned of AMD's legal intentions. Employees, however, didn't always follow the instructions. Intel was compelled to search back-up tapes to produce past email messages. Given that Intel has about 100,000 employees who send and receive dozens of messages each day, the total number of messages in a year processed by Intel may exceed 500 million messages per year. In April 2007, the Wall Street Journal reported that Intel "spent $3.3 million to process computer tapes to help recover missing emails and expects to spend 'many millions of dollars' in the effort."
Deadlines Must Be Met	In Best Buy v. Developers Diversified Realty, the defendants argued that the emails and other electronic documents that were demanded by Best Buy were not "reasonably accessible" from Developers Diversified's back-up system. They cited a cost of $125,000 to recover the information, although they did not substantiate the cost. The judge did not accept the argument and ordered that the information be produced within 28 days, including IT time and legal preparation. According to Law.com, final cost to restore and review the emails and other documents from 345 back-up tapes was an estimated $500,000, not including attorney fees.
Lack of Resources Is Not a Factor	In Williams v. Taser International, one of Taser's representations regarded limited resources in a small organization. Taser represented that it made a significant effort to meet court requirements by hiring and training a technology employee specifically to manage the electronic discovery process. As Taser has just 245 employees, according to its web site, hiring a staff member could be seen as significant. The court, however, did not accept limited resources as an excuse. It stated that it expected the company to make "all reasonable efforts … including … retaining additional IT professionals to search electronic databases and adding additional attorneys ...". This opinion suggests that the courts would not accept a lack of IT resources as a reason for failing to meet the FRCP requirements, even for a small organization.
Failure to Produce is Costly	The financial services firm Morgan Stanley was sued by billionaire financier Ronald Perelman. Morgan Stanley could not reliably produce e-mails for the court. The judge in the case ruled that Morgan Stanley "deliberately" violated her orders. In an uncommon move, the Judge switched the burden of proof to Morgan Stanley, and instructed the jury to determine only if Perelman had relied on Morgan Stanley in the transaction in question. The Jury awarded Ronald Perelman $604.3 million in compensatory damages and $850 million in punitive damages.
Preserving Email Evidence	In United Medical Supply v. United States, the government was sanctioned for allowing email to be deleted. There was not a central archive, so the government needed to depend upon employees following policy. A government attorney properly notified those involved to hold email according to the policy. The problem is that the government did not confirm that all the people involved were actually following the notice. Counsel made representations about what was being preserved based on inaccurate or incomplete IT information. The result was that the court ordered the government to reimburse United Medical Supply for some of their discovery costs and barred them from cross-examining United Medical Supply's expert witness on various aspects at trial.

Electronic Discovery Reference Model (EDRM)[5]

The scope of email eDiscovery can be understood by reviewing eight steps of the EDRM reference model.



1. *Identification*- Understand the "inventory" of email that might be relevant in a particular legal action and that might have to be presented during discovery. At this point in the process, discovery demands, disclosure obligations and other pertinent claims and demands are reviewed and considered. The goal at this stage of the process is to understand the universe of email that might be required in order to respond to appropriate eDiscovery requests and then determine the subset of email that will be relevant for further processing.
2. *Preservation*- This is a critical step that ensures that email is protected from spoliation and modification, such as through the imposition and enforcement of a legal hold on all relevant emails.
3. *Collection* - During this phase, all relevant email is collected from the various sources that contain it, including messaging archives, backup tapes, file servers, desktops, laptops, employees' home computers, smartphones and other sources.
4. *Processing* - At this point, collected data should be de-duplicated in order to reduce the amount of data that must be processed during subsequent phases of the discovery process. Collected data should also be prioritized into a) that content that will likely be relevant later in the process and b) content that will likely not be relevant. At this point, decision makers may want to convert emails into a form that will permit the most efficient and thorough review of its contents.
5. *Review* - The review phase includes redacting email content as appropriate, evaluating the content for its relevance, determining if specific items are subject to attorney-client privilege, etc.
6. *Analysis* - This phase involves a variety of activities, including determining exactly what the email means in the context of the legal action at hand, developing summaries of relevant information, determining the key issues on which to focus, etc.
7. *Production* - The production of data involves delivering the relevant emails and attachments to any parties or systems that will need it. It also includes the activities focused on delivering emails in the appropriate form(s), including DVDs, CD-ROMs, paper, etc.
8. *Presentation* - The presentation of email is a key consideration at various points of the e-discovery process – as information is reviewed, analyzed, produced, etc. The specific forms of presentation for email will vary widely depending on the content; how, where and by whom the content will be presented; and other factors.

[5] *Electronic Discovery Reference Model V2.0 edrm.net*

Regulation, Compliance and Records Information Management

It is estimated that there are more than *35,000* global regulations affecting record management. A few examples of these regulations and agencies include:

- Sarbanes-Oxley Act
- SEC Regulation 240.17-a-4
- Health Insurance Portability and Accountability Act (HIPAA)
- U.S.A. Patriot Act
- Gramm-Leach-Bliley Act
- Anti-Terrorism, Crime, and Security Act (U.K.)
- Fair Labor Standards Act
- Food and Drug Administration (FDA)
- Environmental Protection Agency (EPA)
- Occupational Safety and Health Administration (OSHA)
- Internal Revenue Service (IRS)
- Consumer Product Safety Act
- Employee Retirement Income Security Act (ERISA)
- Personal Information Protection and Electronic Documents Act (Canada)

Organizations must comply with these regulations depending on industry and where they conduct business. Penalties for non-compliance vary dramatically depending on industry, regulation, and regulating body. In order to comply with record maintenance regulations regarding emails an organization must:

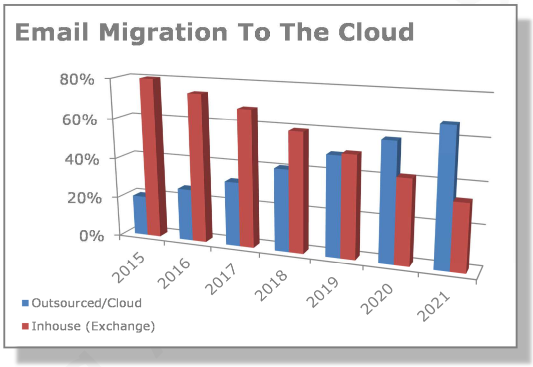
1. Identify what emails, including attachments, must be retained in order to achieve an appropriate level of risk
2. Determine how long these identified emails and associated attachments must be retained and the criteria used for this determination
3. Be able to show that retained emails and associated attachments cannot and have not been altered
4. Be able to produce retained emails and associated attachments in a timely manner as required for compliance audits
5. Determine the appropriate time for destroying retained emails and associated attachments in order to maintain an appropriate level of risk

Information Technology (IT)

Corporate email is a business-critical application essential to internal and external staff, customer and supplier communications, and collaboration. Business operational requirements have traditionally been the main drivers of email solutions provided by Information Technology. By 2012 most organizations had internally implemented Microsoft's Exchange application, sometimes supplemented with an archive solution, to support these requirements.[6]

As the volume, size, and importance of email as a business support tool has grown, the cost and complexity of providing appropriate email service has grown at a time when there is a need to reduce overall IT costs.

These changes, combined with improved cloud-based email solutions, have resulted in a migration to applications such as Microsoft's Office 365 and Google's Google Apps. It is estimated that the majority of business email will be cloud based by 2020.[7]



The legal, risk, and regulatory requirements of email have traditionally been secondary to business operational requirements. The inclusion of email as a potential business record has had major impact on that. Many organizations have created "add-on" IT processes and applications in an attempt to meet these evolving requirements. Typically these "add-ons" were based on data backups of the email application (MS Exchange/archiving) servicing business operations.

Information technology faces a large number of evolving and changing requirements for email including:

- Increased volume
- Larger email size
- More history and easier access to it
- Access anywhere from any device
- Maintenance of legacy email application and processes
- Migration to the cloud
- Growing regulatory requirements
- Rising legal and eDiscovery needs
- Cost reduction pressure
- Increased security needs

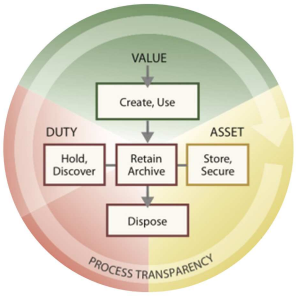
[6] Fortune February 1, 2016 As Big Companies Move Email to the Cloud, Microsoft Shows Strength citing Gardner . Microsoft Exchange Server had more than 80% market share

[7] The Radicati Group, Inc. Microsoft Office 365, Exchange Server and Outlook Market Analysis, 2017 – 2021 and Microsoft Office 365, Exchange Server and Outlook Market Analysis, 2015 – 2019

Processes

Successful email management requires a set of interoperable processes and supporting systems that provide four basic functions:

- *Create and Use*
- *Retain and Archive*
- *Store and Secure*
- *Dispose*



Create and Use

Appropriate use of corporate email should be documented and communicated to all employees. A well communicated email policy helps prevent email threats, since it makes your staff aware of the corporate rules and guidelines, which if followed can help protect your company from:

- *Legal Liability* - In most cases the employer is held responsible for all the information transmitted on or from their systems. As a result, inappropriate emails (i.e. offensive, those containing viruses, etc.) can result in costly penalties.
- *Confidentiality Breaches* - Most confidentiality breaches occur from within the company. These breaches can be accidental, for instance by selecting a wrong contact in the To: field. However, confidentiality breaches can also be intentional. Whether it is by mistake or on purpose, the result of the loss of confidential data is the same.
- *Damage to Reputation* - There is no doubt that the contents of corporate emails reflect on the business. A badly written email, or an email containing unprofessional remarks will cause the recipient to have a bad impression of the company the sender is representing. If an incident does occur, an email policy can minimize the company's liability for the employee's actions.
- *Lost productivity* - In the US, a survey revealed that 86 per cent of workers used their company email to send and receive personal emails. A recent study by the Gartner Group found that unproductive internal emails take up 30 percent of employees' time spent reading email.
- *Network Congestion, Outage and Storage* - Spam and personal use of email can cause a company's email system to waste valuable technical resources (network, processing, and storage), not to mention employees' time.
- *Monitoring* - It is essential to have an email policy that states the possibility of email monitoring. If you do not have such as policy you could be liable for privacy infringement.

Portions of an email policy can frequently be automatically enforced by the email system itself (i.e. retention/deletion). In addition, audits are typically required to ensure the email system and emails contained in it are appropriate.

The following pages provide a typical email use policy for illustrative purposes.

Sample Email Use Policy

The purpose of this policy is to ensure the proper use of [Company]'s email system and make users aware of what [Company] deems as acceptable and unacceptable use of its email system. [Company] reserves the right to amend this policy at its discretion. In case of amendments, users will be informed appropriately.

Email is a business communication tool and users are obliged to use this tool in a responsible, effective and lawful manner:

- *If you send emails with any libelous, defamatory, offensive, racist or obscene remarks, you and [Company] can be held liable.*
- *If you forward emails with any libelous, defamatory, offensive, racist or obscene remarks, you and [Company] can be held liable.*
- *If you unlawfully forward confidential information, you and [Company] can be held liable.*
- *If you unlawfully forward or copy messages without permission, you and [Company] can be held liable for copyright infringement.*
- *If you send an attachment that contains a virus, you and [Company] can be held liable.*

If any user disregards the rules set out in this Email Policy, the user will be fully liable and [Company] will disassociate itself from the user as far as legally possible.

The following rules are to be strictly adhered to:

- *It is strictly prohibited to send or forward emails containing libelous, defamatory, offensive, racist or obscene remarks. If you receive an e-mail of this nature, you must promptly notify your supervisor.*
- *Do not forward a message without acquiring permission from the sender first.*
- *Do not send unsolicited email messages.*
- *Do not forge or attempt to forge email messages.*
- *Do not send email messages using another person's email account.*
- *Do not copy a message or attachment belonging to another user without permission of the originator.*
- *Do not disguise or attempt to disguise your identity when sending mail.*
- *Emails must be deleted within six (6) months*
    - ✓ *Emails that contain information required beyond this time period should be filed in the appropriate corporate repository*
- *Signatures must include your name, job title and company name. The following disclaimer will be added underneath your signature:*

> *This communication and any files transmitted with it may contain information that is confidential, privileged and exempt from disclosure under applicable law. It is intended solely for the use of the individual or entity to which it is addressed. If you are not the intended recipient, you are hereby notified*

that any use, dissemination or copying of this communication is strictly prohibited. If you have received this communication in error, please notify the sender.

- *Although [Company]'s email system is meant for business use, [Company] allows the reasonable use of email for personal use if certain guidelines are adhered to:*
  - ✓ *Personal use of email should not interfere with work.*
  - ✓ *Personal emails must adhere to the guidelines in this policy.*
  - ✓ *Personal emails must be deleted within five (5) business days.*
  - ✓ *The forwarding of chain letters, junk mail, jokes and executables is strictly forbidden.*
  - ✓ *All messages distributed via the company's email system, even personal emails, are [Company]'s property.*

You must have no expectation of privacy in anything you create, store, send or receive on the company's computer system. Your emails can be monitored without prior notification if [Company] deems this necessary. If there is evidence that you are not adhering to the guidelines set out in this policy, the [Company] reserves the right to take disciplinary action, including termination and/or legal action.

All email accounts maintained on our email systems are property of [Company]. Passwords should not be given to other people and should be changed at least once every six (6) months. Email accounts not used for 60 days will be deactivated and possibly deleted.

If you have any questions or comments about this Email Policy, please contact your supervisor. If you do not have any questions [Company] presumes that you understand and are aware of the rules and guidelines in this Email Policy and will adhere to them.

DECLARATION

I have read, understand and acknowledge receipt of the email policy. I will comply with the guidelines set out in this policy and understand that failure to do so might result in disciplinary or legal action.

Signature: ______________________________ *Date:* ______________________

Printed Name: ______________________________

Retain and Archive

Retention of email is a cost/benefit/risk decision that is unique to a company and the industry(s) and geography(s) that it participates in.

- *Computer systems and infrastructure supporting email and related applications*
- *Business, Administrative, and Information Technology personnel costs to use and support email processes and systems*

Cost
Risk
Benefit

- *Inability to adequately manage litigation costs and outcomes*
- *Fines and penalties associated with regulatory non-compliance*

- *Access to email records required for regulatory compliance and audits*
- *Access to email records required to comply with litigation demands*
- *Access to email records utilized in business operations*

How a company interprets these cost/benefit/risk forces should be reflected in a documented email retention policy.

Email Retention Approaches

There are two major email retention approaches that can be readily implemented today. The first is based on journaling. Email journaling captures all emails coming into, going out of, and moving within an email system. Different email systems have different journaling capabilities.[8] The second approach is based on records declaration by the user. The second requires users to declare that an email is a record by moving or copying it to a separate location for retention.

Available approaches and capabilities are dependent on the email system(s) in use at an enterprise.

[8] *Journaling is different than archiving. Journaling maintains a copy of all communications. Archiving refers to reducing the strain of storing emails within the production system by moving emails from the production system into a secondary repository for retrieval as required.*

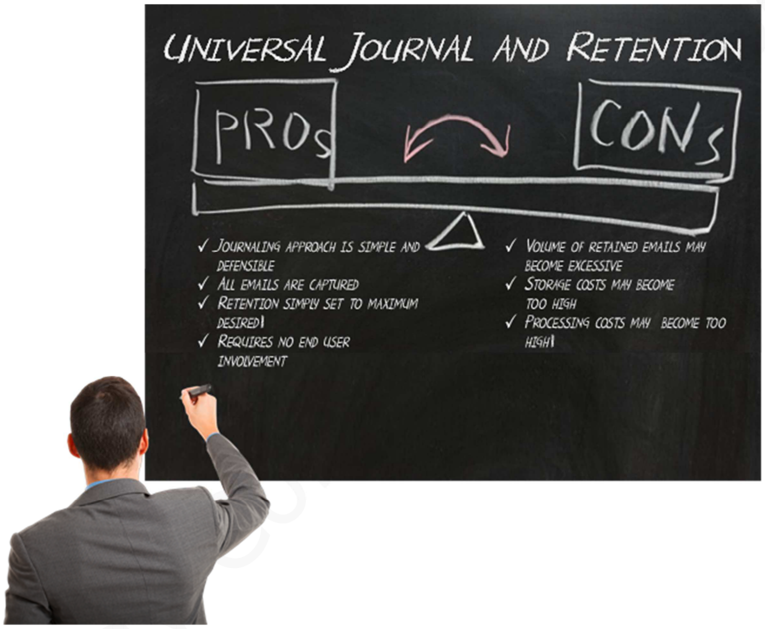
Many companies make the mistake of believing that email backups, taken for disaster recovery purposes, are a valid journaling approach. Unfortunately, email backups do not contain emails that were fully processed during the day (received and/or sent that day, then deleted by the user). These processed emails may still exist outside the organization! Additionally, if emails have not been processed by the user, the same email will be in multiple backups. This increases the resources required to locate particular emails in response to audit or eDiscovery requests.

Journaling

There are a number of email journaling approaches, typically a variation of one of the following:

- Universal journal and retention where every email in the system is captured and retained for a fixed period of time
- Role-based journal and retention where emails are captured and retained for a time period based on an individual's role in the enterprise
- Universal journal and role-based retention where all emails are captured but retention periods are based on an individual's role in the enterprise

The costs and capability to implement these approaches is highly dependent on the email system(s) used by the enterprise.[9]



UNIVERSAL JOURNAL AND RETENTION

PROS

CONS

✓ JOURNALING APPROACH IS SIMPLE AND DEFENSIBLE
✓ ALL EMAILS ARE CAPTURED
✓ RETENTION SIMPLY SET TO MAXIMUM DESIRED!
✓ REQUIRES NO END USER INVOLVEMENT

✓ VOLUME OF RETAINED EMAILS MAY BECOME EXCESSIVE
✓ STORAGE COSTS MAY BECOME TOO HIGH
✓ PROCESSING COSTS MAY BECOME TOO HIGH!

TCA believes:

- The universal journal and retention approach is best suited for small to mid-sized businesses. It provides the basis for a straightforward and simple retention policy while ensuring that compliance and legal requirements are met. It can become cumbersome for larger organizations due to the volume of emails that can be involved.
- The role-based journaling and retention approach is viable if the enterprise email system readily supports it. However, it may be difficult to determine whose emails should be journaled, especially for eDiscovery purposes.
- Until technology develops that allows for automated content-based email retention, the universal journal and role-based retention approach is the most appropriate strategy for all but the smallest of companies. It provides the basis for a defensible retention policy and a reduction in the overall amount of retained email without requiring user involvement or education.

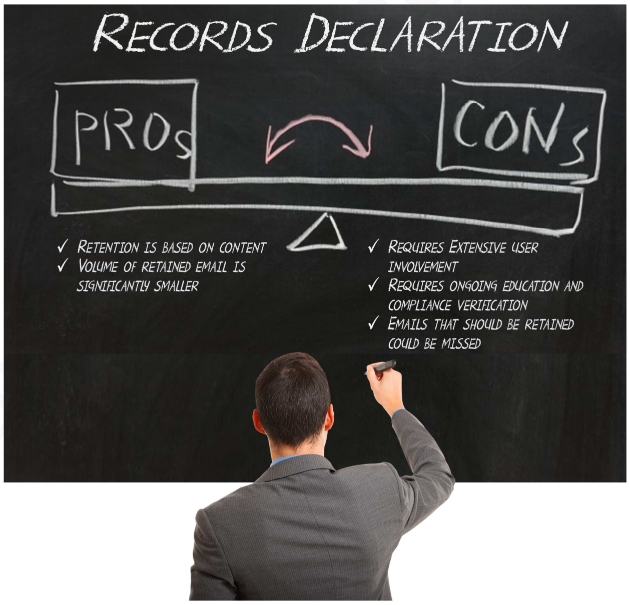
[9] *External hardware devices and software solutions are also available for email journaling*

Records Declaration

The records declaration email retention approach has long been the favorite of compliance and records management personnel because it gets to the basic retention issue: what determines whether an email is a business record is its content. Using this approach, the content of an email dictates whether it is retained and for how long.

Unfortunately, today's technology is not capable of supporting a valid and defensible automated method for reviewing the content of an email to determine if, and for how long, an email should be retained. Instead, the email user must declare an email as a record by manually reviewing and filing it for appropriate retention.

Many electronic records management vendors provide the capability for users to file their emails into appropriate repositories for retention purposes. Some are integrated with mail clients, such as MS Outlook, providing a simple click and drag to a folder interface.


RECORDS DECLARATION
PROs
CONs
✓ RETENTION IS BASED ON CONTENT
✓ VOLUME OF RETAINED EMAIL IS SIGNIFICANTLY SMALLER
✓ REQUIRES EXTENSIVE USER INVOLVEMENT
✓ REQUIRES ONGOING EDUCATION AND COMPLIANCE VERIFICATION
✓ EMAILS THAT SHOULD BE RETAINED COULD BE MISSED

TCA believes:

- Although the records declaration approach for email retention has long been advocated by software vendors and compliance officers, it is almost impossible to effectively and efficiently implement across an organization of any size and scale. The training required to educate email users on what should be retained and for how long, combined with the daily effort required to manually process email and extensive compliance verification efforts, make this approach infeasible for most companies.

Retention Policy

A company's email retention process is a cost/benefit proposition. The driving forces behind email retention are:

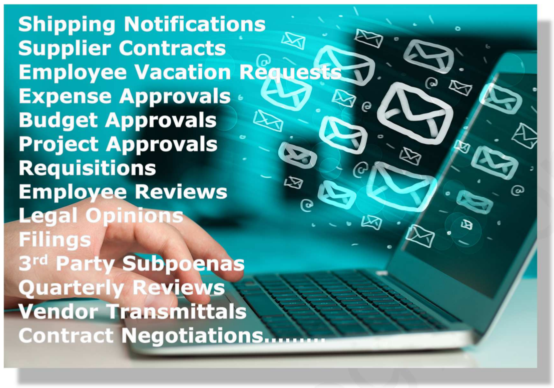
- the benefit of having email records required for regulatory compliance and audits
- the benefits of having the information to comply with potential litigation demands

versus

- the costs associated with retaining and managing archived email
- the costs associated with the inability to provide adequate discovery during litigation
- the costs associated with lack of regulatory compliance

How a company interprets those forces should be reflected in a documented email retention policy.

Email retention policies vary from extremely complex, attempting to address all the rules and regulations that can apply to a company's business records, to declaring that email contains no business records.



While a company may wish that its corporate email system contained no business records, what determines whether an email is a business record is its content. If a company develops an email retention policy that states that their corporate email contains no business records, regulators and courts are likely to take a very different view!

TCA believes:
An appropriate strategy is to develop and document an email retention policy that is:

- *Defensible* – takes into account basic regulations and laws that effect the company
- *Consistently Enforced* - can be demonstrated to be consistently and accurately carried out
- *Simple and Straightforward* – uses broad categories to cover retention requirements within a manageable number of retention archives

A sample Email Retention Policy is presented on the following page based on a universal journaling and role-based retention strategy.

Sample Email Retention Policy

Purpose

This policy establishes standards for the retention of electronic mail, "email", stored centrally [Company]'s email servers.

Scope

This policy applies to the following:

- *All electronic mail systems and services and records provided or owned by [Company].*
- *All users of [Company]'s email services, including:*
  - ✓ *Full and part-time employees;*
  - ✓ *Contractors authorized to use [Company]-owned equipment or network resources;*
  - ✓ *Volunteers who have been provided with an email account/service; and*
  - ✓ *All other users of [Company]'s information technology resources.*

Policy Details

Background

Email is an efficient and timely communications tool that is provided by the [Company] to its employees, contractors, and volunteers to assist them in supporting [Company] functions and conducting [Company]'s business within its own organization, with government and private business partners, and with the public. [Company] maintains the email system and servers and performs limited storage of email on backup tapes, solely for disaster recovery purposes.

Retention of email on [Company]'s servers and backup tapes may assist [Company] staff in performing their duties, but excessive retention of mail in the email system will compromise system performance. We must manage [Company]'s email servers using software that limits the storage of individual mailboxes, in order to operate [Company]'s enterprise email function within email budget constraints, to ensure consistent reliable email system performance and fail-over capability, and to ensure reliable, available emergency services. This policy defines email retention parameters designed to permit reasonable email retention while ensuring a system that performs consistently and reliably with full failover capability.

Operational Email Retention

All email residing on [Company]'s email servers will be stored for six months (180 days). All email bearing a date older than six months—regardless of agency, sender, recipient, or any other attribute--will be deleted automatically and permanently from the [Company]'s email system. This deleted email will not be retained on any media or log. Full backups of emails on the system will be taken each week and stored on electronic media. These backups will be kept for three weeks at which time the electronic media will be re-utilized. As a result, the maximum "age" of any email that may be recovered from the [Company]'s email system will be 201 days (six months plus three weeks).

Email Record Retention

All emails processed by [Company]'s email system will be recorded and maintained as records outside of the operational email system for legal and compliance purposes. Email records will be preserved according to the following schedule:

Department/Role	Retention Period
Executive	10 Yrs
Human Resources/Director and Above	7 Yrs
Finance/Director and Above	7 Yrs
Customer Service	3 Yrs
Sales	3 Yrs
Legal	10 Yrs
Procurement/Director and Above	5 Yrs
Manufacturing	1 Yrs
Research & Development	7 Yrs
All Others	1 Yr

Access to these records will be limited to those individuals that require access to perform their assigned functions.

Requests for Extended Preservation

Notwithstanding the general rules above, any department may designate specific emails for preservation beyond the general preservation limit. [Company] will fulfill any request for such extended preservation as long as the request: 1) is made in a written communication, 30 days before the end of the general preservation limit, from the department director and the General Counsel; 2) specifies the preservation period; 3) specifies the business and/or legal purpose for the preservation; and 4) identifies specifically the email to be preserved by any or all of the following: mailbox user name(s), message recipient(s), message sender(s), date range(s), and message/attachment text term(s).

Store and Secure

Once an email has been retained, it is an asset that needs to be stored and secured.[10] Different regulations, industries, and companies have different storage requirements for electronic records such as email, however there are a few basic requirements involving the legal defensibility and technical performance of the storage solution:

- *Immutable* - Emails must be stored using a method that does not allow modification (i.e. immutable). The ability to modify or delete stored emails must be prevented by the storage container. Some industry regulations have historically required that electronic business records be stored on Write Once, Read Many (WORM) media.
- *Accessible* - Stored emails must be readily accessible. Ready access to stored emails is required in order to respond in a timely manner to legal discovery and compliance audit requests.
- *Scalable* - Email storage repository must be scalable. One of the unique problems of email business records is the sheer volume of information that email represents. Retaining emails over the span of years can easily require terabytes of storage for even a small to mid-sized business.
- *Secure* – Access to stored emails must be limited to those individuals that have valid business reasons to view them. Not only should access be controlled, but ideally all access to stored emails should be recorded and logged.

TCA believes:

- Access requirements, and the declining cost of storage, have driven modern electronic document retention towards online storage solutions.
- Enterprises should look for Commercial Off-The-Shelf (COTS) solutions for electronic records storage.
- Securing access, although always a requirement of good electronic records management, is becoming more important.
- Email is typically the largest volume of electronic document storage within an overall records management solution for an enterprise and its storage and security requirements should be a major consideration in any electronic records management solution.

[10] *DoD 5015.02-STD ELECTRONIC RECORDS MANAGEMENT SOFTWARE APPLICATIONS DESIGN CRITERIA STANDARD April 25, 2007 contains comprehensive requirements for electronic record storage*

Discovery and Hold

Emails are retained and stored in order that the information contained within the message and its associated attachments is available to respond to compliance audits or legal discovery requests.[11] Email discovery and audit requests typically are based on:

- message sender(s)
- message recipient(s)
- date range(s)
- message/attachment text term(s)

Locating appropriate emails in a timely manner can be a challenge because of the volumes that are typically involved.

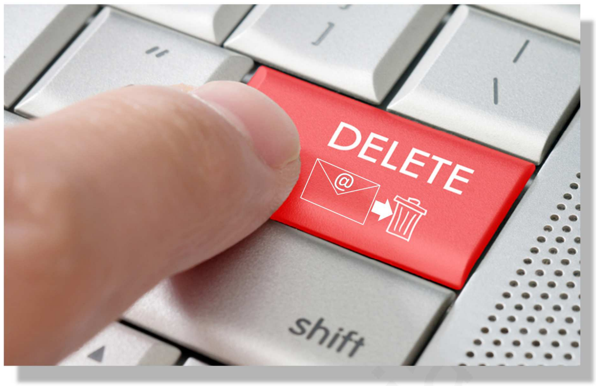
After stored emails have been "discovered" in response to a legal or compliance need, they need to be preserved until the legal or compliance need has been satisfied. This requires the ability to override the normal retention policy for those emails, ensuring they are not destroyed.

TCA believes:

- Utilizing a storage solution that does not provide an efficient and effective way to search through stored emails and retain those required for legal discovery and/or compliance audits can add significantly to the cost of compliance efforts associated with email.
- Only the smallest businesses should consider using multiple sequential files (i.e. tape files) to store retained emails because of the processing costs and time required to discover and hold individual emails.
- There are a large number of Commercial Off-The-Shelf (COTS) solutions available for Discovery and Hold functions that should be considered prior to developing a custom solution.

[11] Archiving email for business operational purposes, so users can locate information that assist them in performing their business tasks, is a different function that must be considered when designing the overall email records management process. Emails that are in an operational archive must be in the email records management store. If an email needs to be retained beyond typical records management timing for operational purposes it should be moved from the email operational archive into a managed store.

Dispose



A fundamental principle of electronic records management according to the Sedona Conference[12] is that if an organization has implemented a clearly defined records management program specifying what information and records should be kept for legal, financial, operational, or knowledge-value reasons, and has appropriate retention systems and/or periods, then information not meeting these retention guidelines can and should be destroyed.

When a stored email has reached the end of its retention period based on policy and associated schedules, it must be destroyed. A fundamental legal problem can, and will, arise if proper email record destruction processes are not established and enforced. Morgan Stanley lost a billion dollar lawsuit on the basis of old back-up tapes being found in storage after the trial's discovery process was closed.

It is important to include IT operational data (i.e. backups and operational archives) in the email record destruction process so that no copies of the email remains past it retention period.

TCA believes:

- The large volumes associated with email record management dictate the use of some form of automation around the disposal process to ensure the retention policy is enforced.
- Emails that exist outside the electronic records management storage environment must be considered when designing the overall email disposal strategy.

[12] *The "Sedona Principles" (www.sedonaconference.org) is an attempt by the legal profession to establish a guideline for lawyers, records management, and information technology professionals for best practices in managing information records. These principles are becoming the recognized records-management rules that courts are relying on to determine proper legal discovery compliance.*

Implementing eMail Record Management

Email Record Management Planning

Planning for email record management must include at least three parties:

1. Business users who need information located in email to operate the organization
2. Legal, risk, and regulatory departments who understand the organization's duty to preserve the information located in email beyond its immediate business value
3. IT departments who must implement the mechanics of email management legal, compliance, and information technology.

Just like filing is an adjunct activity to one's work, records management in and of itself is not a core business application. Records management should support core business processes without being intrusive in order to be truly effective.

Since the volume of email records can easily be an order of magnitude greater than all other electronic records combined, email record management should be a major consideration within an overall records management strategy.

TCA believes:

- Email record management should be considered as part of an overall record management strategy.
- A records management strategy should include:
  - Scope
    - ✓ FRCP
    - ✓ RIM Standards (ISO 15489)
    - ✓ Electronic Communications (ANSI/ARMA 9-2003)
    - ✓ Sedona Guidelines
    - ✓ Federal Sentencing Guidelines (Compliance Program)
    - ✓ Industry regulations
  - Operating Model
    - ✓ Key activities
    - ✓ Responsibilities
    - ✓ Interfaces
  - Needs Assessment
    - ✓ Business model and functions inventory
    - ✓ Policy list
    - ✓ Process list
    - ✓ Procedure list
  - Enabling IT Infrastructure and Services
  - RM Program Plan
    - ✓ Schedule
    - ✓ Costs
    - ✓ Resources

COTS

There are a large number of record management solution vendors in the marketplace today that handle email. The core of any system developed and implemented should be based on one, or a combination, of these solutions.

The amount of effort required to implement an email record management solution can vary widely depending on the "out-of-the-box" capabilities of the COTS solution(s) selected, the email system in use, the records management strategy of the company, and specific requirements for email record management based on the company's industry and policies.

The marketplace for email record management solutions has experienced a great deal of consolidation over the last few years. This consolidation is continuing as large companies are acquiring small point vendors and integrating the products into their overall product portfolio. Email record management solution vendors can be categorized into four general groups:[13]

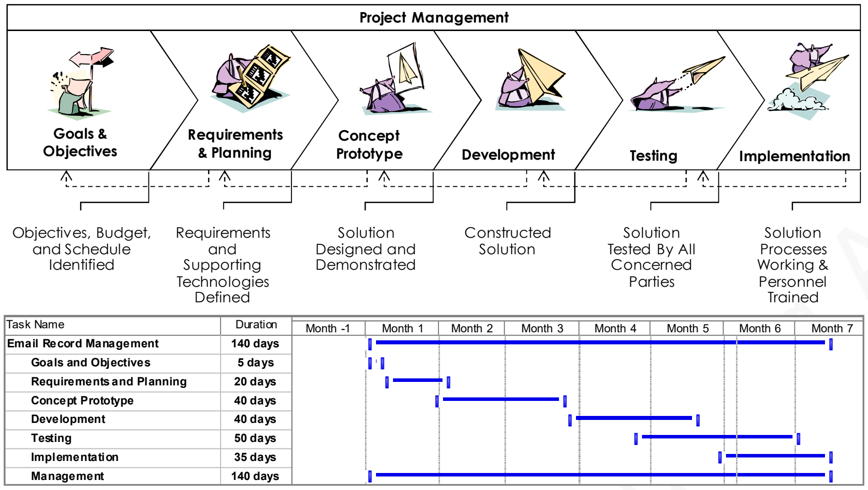
1. ECM Vendors[14] - applications that manage enterprise content that will also manage emails records. Examples would include:
   - ✓ Opentext
   - ✓ IBM Content Collector
   - ✓ MS SharePoint
2. Storage Management Vendors – applications that have typically grownup around reducing the storage requirements of mail servers to improve operational performance. Examples would include:
   - ✓ Veritas Enterprise Vault
   - ✓ HP Integrated Archive Platform
   - ✓ Barracuda Networks Message Archiver
3. Hosted or Outsourced Service – services that provide email archive and management via the "cloud". Examples would include:
   - ✓ Sonasoft SonaCloud
   - ✓ Smarxh Email Archiving
4. "Pure play" vendors – software designed specifically to provide record management
   - ✓ ZipLip Inc's ZL Unified Archive
   - ✓ Iron Mountain's NearPoint for Microsoft Exchange Server

[13] *Due to rapid market changes specific examples will be out of date when this paper is read. Enterprises should review the current state of the market based on their unique requirements and strategy when determining what vendors may satisfy their needs.*

[14] *Major ECM vendors include Alfresco, Dell EMC, Everteam, Hyland, IBM, Laserfiche, Lexmark, M-Files, Microsoft, Newgen Software, Objective, OpenText, Oracle, SER Group, and Xerox*

Methodical Development and Implementation

Project methodology models can be described along a spectrum of agile to iterative to sequential. Agile methodologies, such as XP and Scrum, focus on lightweight processes which allow for rapid changes along the development cycle. Iterative methodologies, such as Rational Unified Process and Dynamic Systems Development Method, focus on limited project scope and expanding or improving products by multiple iterations. Sequential or big-design-up-front (BDUF) models, such as Waterfall, focus on complete and correct planning to guide large projects and risks to successful and predictable results.


Project Management
Goals & Objectives
Requirements & Planning
Concept Prototype
Development
Testing
Implementation
Objectives, Budget, and Schedule Identified
Requirements and Supporting Technologies Defined
Solution Designed and Demonstrated
Constructed Solution
Solution Tested By All Concerned Parties
Solution Processes Working & Personnel Trained
Month -1
Month 1
Month 2
Month 3
Month 4
Month 5
Month 6
Month 7

Task Name	Duration
Email Record Management	**140 days**
Goals and Objectives	**5 days**
Requirements and Planning	**20 days**
Concept Prototype	**40 days**
Development	**40 days**
Testing	**50 days**
Implementation	**35 days**
Management	**140 days**

The steps outlined in this graphic and associated work plan represent the efforts required to implement email record management utilizing a Waterfall methodology

This sample work plan is typical of a mid-sized company implementation of email record management[15]. Projects typically vary from three (3) months to three (3) years depending on the size and complexity of the enterprise. Resource staffing and effort estimates will vary, primarily based on:

- ✓ Retention policy
- ✓ Retention approach
- ✓ Industry requirements
- ✓ Conversion requirements
- ✓ Software/hardware selected
- ✓ Overall electronic records management strategy and related strategy
- ✓ Number of email users
- ✓ Complexity of the email infrastructure

TCA believes:

- Whatever management methodology is utilized, it is extremely important to utilize a structured approach to the implementation of email record management in order to be successful.

[15] A more detailed free WBS and work plan can be requested via TCA's website at http://www.tca-llc.com/contactus/contactus.aspx

Insights

- Emails are a business records and need to be managed to avoid extensive business risk
- Email record management must take into account the needs of:
  - The overall business use of email within the enterprise
  - Legal, risk, and regulatory needs of email records
  - Information technology capabilities and costs associated with email, and overall electronic, records management
- Companies need a clearly communicated email use policy
- Companies need a documented email retention policy that takes into account the ability to implement it
- Email journaling is recommended as the best means to retain emails based on the current state of technology and typical records management requirements
- Email record management is only part of an overall electronic records management strategy and solution
- Email records management solution development should follow a methodical approach utilizing off-the-shelf solutions as much as possible

How TCA Can Help

TCA works with companies to define, plan, and implement changes that improve the performance of their business. We can help plan and implement appropriate Email Record Management strategies for your company.

Typical TCA Email Record Management services include:

- ✓ Assisting customers create Email Use and Retention Policies
- ✓ Working with customers to develop the appropriate email and overall record management strategy
- ✓ Supporting customers’ vendor selection, negotiation, and contracting process for Email record management software, hardware, and services
- ✓ Providing project resources as required by the customer to plan, develop, and implement Email and overall record management solutions

For more information about how TCA can help your business please contact us

Mail	**P.O. Box 420076** **Atlanta, GA 30342**
Phone	**404.303.1795 x142** **877.842.1842**
Fax	**404.943.9081**
Email	**RecordMgt@tca-llc.com**

Visit us at www.tca-llc.com