The Sedona Conference Journal

Volume 8 2007

The Sedona Conference Commentary on Email Management: Guidelines for the Selection of Retention Policy

The Sedona Conference

Recommended Citation: The Sedona Conference, *Commentary on Email Management: Guidelines for the Selection of Retention Policy*, 8 SEDONA CONF. J. 239 (2007).

For this and additional publications see:
https://thesedonaconference.org/publications

THE SEDONA CONFERENCE® COMMENTARY ON EMAIL MANAGEMENT: GUIDELINES FOR THE SELECTION OF RETENTION POLICY

*A Project of The Sedona Conference® Working Group on Electronic Document Retention and Production, eMail Management and Archiving Special Project Team**

Editor: Thomas Y. Allman

[REVISED April 7, 2007]

Electronic mail ("Email") is of vital importance to the productive efforts of an enterprise and its use is growing exponentially. In 2005, the average user processed 75 e-mails a day and the Radicata Group estimates that corporate e-mail traffic per user has increased at a rate of 33% per year since then. Projections are that worldwide traffic in 2006 was at the rate of 183 billion messages per day.[1]

Many organizations are struggling to decide how to best cope with the explosion of email while reconciling competing needs imposed by business, regulatory and litigation requirements. This Sedona Conference® Commentary suggests Guidelines for determining the core elements of an email retention policy suitable for public and private entities. Although the legal, regulatory and cultural environment of each organization varies greatly, there are common elements to a legally defensible email management policy.[2] In our Working Group discussions, we have been struck by the fact that entities of comparable size with similar legal risk and regulatory profiles can and do successfully adopt different retention strategies and that these strategies can vary over time, depending upon the phase of development, the size and complexity of the organization, and the particular issues most significant to the entity at any particular time.

The key is to develop and enforce in good faith those reasonable policies which best fit the entity.

The Appendix to this Commentary includes a flow chart of the decision making process and also describes two contrasting retention strategies that can be followed.

I. SEDONA GUIDELINES ON EMAIL POLICY DEVELOPMENT

Guideline 1: Email retention policies should reflect the input of functional and business units through a team approach and should include the entire organization including any operations outside the United States.

* Special thanks go to all the WG1 members and observers who provided valuable input and feedback. This document is for educational purposes only and is not a substitute for legal advice. The opinions expressed herein are consensus views of the editors and authors, and do not necessarily represent the views of any individual participants or authors or any of the organizations to which they belong or clients they represent, nor do they necessarily represent official views of The Sedona Conference®.

1 According to Radicati Group, the average size of email messages is also increasing, which, when combined with increased email volume, led to an increase in bandwidth storage requirements per user on the order of 61% per day from 2005 to 2006.

2 We confine our recommendations to the retention of email in its traditional sense, i.e., in its role as a means of electronic communication, often with attachments. We do not here evaluate or discuss the retention policies involved in the use of instant messaging, VoIP or other forms of electronic communication, many of which face similar issues as their useage grows.

Guideline 2: The team should develop a current understanding of email retention policies and practices actually in use within the entity.

Guideline 3: An entity should select features for updates and revisions of email retention policy with the understanding that a variety of possible approaches reflecting size, complexity and policy priorities are possible.

Guideline 4: Any technical solutions should meet the functional requirements identified as part of policy development and should be carefully integrated into existing systems.

II. INTRODUCTION: FRAMEWORK FOR POLICY DEVELOPMENT

A. General Retention Considerations

A business or public entity has the responsibility and authority to determine how best to utilize and retain information managed by its email system. This includes decisions on the specific features which impact the duration of retention of email (hereinafter collectively referred to as "email retention policies"). *See The Sedona Guidelines: Best Practice Guidelines & Commentary for Managing Information & Records in the Electronic Age* (Sedona Conference Working Group Series, September 2005)(hereinafter "Sedona Guideline No. ____"), *Guideline No. 3* ("An organization need not retain all electronic information ever generated or received.").[3] An email retention policy may exist independently of other types of retention policies or it may be part of an umbrella policies relating to retention of information, sometimes known as "records" or "document" management policies.

Whatever their form, email retention policies must be reasonable in purpose and reasonable as applied. They must take into account any applicable statutory and regulatory mandates that may directly or indirectly govern the management of email and, regardless of those requirements, the policy must recognize the need to preserve and produce information sought in legal proceedings.

For example, the financial services industry is notable for the detailed regulations which impact the operation of information systems and mandate technical features (e.g., communications must be retained in a non-rewriteable, non-erasable format).[4] State, federal and local public entities are often also required to manage information created by or received on email systems in accordance with specific regulations created for that purpose.[5]

B. Typical Retention Features

Email retention policies in use today frequently include some or all of the following features to maintain efficient operations. The features are not listed in any particular order based on frequency of use or efficacy in achieving their intended purpose. The focus is on management of email on active sources accessible to users[6] within a firewall which provides appropriate security, virus protection and reasonable spam protection.

1. User Mailbox Size Limitations ("Quotas")

Limitations or "quotas" on the amount of storage space on the network available to an individual user has historically been a principal feature of email management. In a 2005 Industry

3 This principle has been endorsed by the Supreme Court in *Arthur Andersen LLP v. United States*, 544 U.S. 696, 704 (2005)(document retention policies are "common in business" and may be used to explain - and justify - the loss of information in appropriate circumstances).

4 *See* SEC Release No. 34-37182 (May 1996). SEC Release No. 34-38245 (Jan. 1997). NASD Rule 3110, Henry L. Judd and Benjamin S. Hayes, *Records Management of E-Mail by Securities Firms: Legal and Compliance Technology Issues. See, e.g.*, 17 CFR Section 240.17a-4 (originals of all communications received and copies sent by members and broker or dealers relating to its business as such must be maintained for not less than six years, the first two years in an easily accessible place).

5 *See, e.g.*, 36 CFR Section 1234.24 Subpart C *Standards for Managing Electronic Mail Records.* Generally, Federal records are managed within a recordkeeping system and similar provisions exist at state and local levels. *See* Peltz, "Arkansas's Public Record Retention Program: Finding the FOIA's Absent Partner," 28 U. Ark. Little Rock L. Rev. 175 (2006).

6 Email which may be found on media retained for disaster recovery purposes is typically not subject to email retention policies of the type discussed herein. Any indication that backup media is routinely utilized as an unofficial archive should raise questions and call for greater analysis and review. *See* The Sedona Principles: *Best Practices Recommendations & Principles for Addressing Electronic Document Production*, Comment 5.b (July 2005 Version) ("Organizations that use backup tapes for archival purposes should be aware that this practice is likely to cause substantially higher costs for evidence preservation and production in connection with litigation.").

Survey, over one half of the respondents reported that they were "managing" email retention by limiting mailbox sizes. See Electronic Communication Policies and Procedures: A 2005 Industry Study, AIIM & Kahn Consulting, Inc.

Implementation of quotas can vary widely. Typically, a user is given a warning before email is deleted, although the ability to send or receive email may be automatically disabled pending voluntary reduction below the size limits.

2. Automatic Deletion of User Mailbox Contents

Many entities provide for the automatic deletion of email after it has been retained for a certain duration (usually measured in days). Typically, an automatic deletion policy is coupled with options so that the user can move email of significance to an appropriate alternative storage location. In some instances, users are required to print and file copies of email and attachments into an (existing) records management system. Some organizations require users to assign individual retention durations to email as part of the process of classification. The process may be accomplished by "drag and drop" into a networked file with a predetermined retention duration or by making choices from drop down screens. Yet another approach is to delegate the responsibility to the user to set up and use a local file structure which mimics existing records retention schedules for that particular unit.

Automatic classification of email by content using computer generated criteria is not yet a proven technique for managing retention.[7]

Certain types of email content (such as that relating to contracts, regulatory files, trade secrets, and critical business records) may be sufficiently important that dedicated electronic content management repositories are also made available. *See* Cohen, "A Practical Enterprise Methodology for Addressing the Compliance Challenges of eDiscovery, eRetention Management and Defensible Disposition," EMC Corporation (2006).

3. Extended Storage Options

Some entities provide extended capacity or archival storage for undeleted or unallocated email. Email not deleted by a user within a certain period may thus be saved for a long period, with decisions on moving individual email (via declaration as a "record") to records management postponed to another day.

(It should be noted that there may be instances where an entity decides to save all inbound and outgoing email without granting the user the right to winnow out transitory or other information deemed unworthy of retention).

Entities providing extended storage typically move email from active servers to lower cost ("tiered") storage that offer capacities such as de-duplication of messages and attachments in order to reduce server usage. A variation on this approach is to place email into a "vault" or "safe" where the user cannot change or delete the information but can continue to access it for individual use. This increases the likelihood that the information will be accessible when needed. Advocates of this approach also argue that implementation of litigation holds involving large numbers of custodians can be more easily and uniformly managed by use of this feature.

Some entities confine this strategy to specific groups – such as scientists, executives, accountants and HR representatives – because their information predictably may be needed for future business or regulatory inquiry.[8] For these groups, an outer limit of retention may be established based on the various regulatory and business retention requirements. These requirements stem from a large

7 *See* Frazier [Renew Data] and Brownlee, "E-Mail Management Software: The Panacea We've All Been Waiting For?," Pike & Fisher Digital Discovery & e-Evidence," (2006)(pointing out that automatic classification is also being deployed).

8 This approach is mandated in some industries, such as the financial services industry. Radicati Group reported in mid-2006 that 46% of its respondents in a corporate survey were deploying some form of archiving system and that an additional 39% of those without one were planning to deploy one in the future.

and complex series of statutes and regulations (such as tax, employee relations, payroll and benefits, environmental, etc.) as well as common-law and other business requirements.

A variety of practices exist in regard to assigning retention periods. Some entities require that users utilize existing records schedules. Others develop highly simplified versions of their records schedules (a "big bucket" approach) specifically for individual email based on content. Others assign uniform, long term retention periods to all email for classes of users or departments without individual classification on the theory that individual classification is not practicable.

4. Restrictions on Local Storage

Some entities prohibit users from placing information on local PC hard drives (or other distributed devices) to avoid the problem that local hard drives cannot be accessed by others and are not backed up. Eliminating this option can be controversial, since some users may regard local storage as an essential element of their productive use of the information and may not appreciate having to rely upon networked or shared storage.

B. The Importance of Litigation Holds

A good faith and reasonable effort to implement a "litigation hold" to preserve potentially discoverable information needed for litigation or governmental investigations must be made once a preservation obligation is triggered.[9]

Email retention policies which impact on retention must take this imperative into account. *See generally* Sedona Guideline 5 ("An organization's policies and procedures must mandate the suspension of ordinary destruction practices and procedures as necessary to comply with preservation obligations related to actual or reasonably anticipated litigation, government investigation or audit").

Courts have not hesitated to impose sanctions where email was destroyed or lost at a time when a preservation obligation was in effect.[10] Generally, courts have "broad discretion in choosing an appropriate sanction for spoliation," but "the applicable sanction should be molded to serve the prophylactic, punitive, and remedial rationales underlying the spoliation doctrine." *Silvestri*, 271 F.3d at 590 (quoting *West v. Goodyear Tire & Rubber Co.*, 167 F.3d 776, 779 (2nd Cir.1999)).

The 2006 Amendments to the Federal Rules of Civil Procedure ("the Amendments")[11] do not specially spell out when or how a preservation obligation with respect to email is triggered nor do they identify the exact scope of the duty and how it is to be satisfied. Parties are instead encouraged by Rule 26(f) to assess and discuss preservation issues early and Rule 37(f) provides for limited protection from some spoliation sanctions based on the presence of "routine, good faith" operations of information systems.[12]

It is clear from the Rules and the emerging case law that the implementation of litigation holds involving email will receive heightened scrutiny.[13] Reasonable care must be taken in administering a litigation hold to ensure that routine features which may interfere with preservation are addressed.[14]

---

9 The elements of a litigation hold process in the employment litigation context were discussed in detail in *Zubulake v. UBS Warburg*, 229 F.R.D. 422 (S.D. N.Y. 2004) ("Zubulake V"). The principles applicable to a governmental regulatory action are similar to those in the civil context. *See* Cutler, Stegman & Helms, "Document Preservation and Production in Connection with Securities and Exchange Commission Investigations and Enforcement Actions," 37th Annual Institute on Securities Regulation, 1517 PLI/Corp 579, 593 (2005) ("Retention Mechanics").

10 For example, in *Broccoli v. Echostar*, 229 F.R.D. 506 (D. Md. 2005), a defendant that had failed to suspend an automatic deletion process upon being placed on reasonable notice of litigation was found to have engaged in spoliation.

11 The Amendments to the Federal Rules of Civil Procedure went into effect on December 1, 2006. *See* http://www.uscourts.gov/rules/EDiscovery_w_Notes.pdf.

12 *See* Allman, "Defining Culpability: The Search For a Limited Safe Harbor in Electronic Discovery," 2006 Fed. Cts. L. Rev. 7, *available at* http://www.fclr.org/2006fedctsrev7.htm.

13 *See Cache La Poudre Feeds v. Land O'Lakes*, Civil Action No. 04-cv-00329-WYD-CBS, 2007 WL 684001 (March 2, 2007)(sanctioning producing party for failing to meet ongoing preservation obligations).

14 *Miller v. Holzmann*, CA No. 95-01231 (RCL/JMF), 2007 WL 172327 (D.D.C. January 17, 2007)(a litigation hold can help prevent destruction of information where a computer is programmed to destroy information after a period of time or where a person unaware of litigation may destroy electronically discoverable information).

The email retention policy may leave the specific details of litigation hold implementation to other policies and procedures, including ad hoc processes, but it is important that the entity be able to demonstrate that email retention practices are actually subject to the constraints imposed by preservation obligations as they arise. A companion Sedona Commentary to this paper is currently being prepared to address the considerations involved in establishing and implementing litigation holds.

III. DISCUSSION

Guideline 1: Email retention policies should reflect the input of functional and business units through a team approach and should include the entire organization including any operations outside the United States.

Commentary:

Until recently, the management of email was viewed primarily as a technology issue to be handled by the IT department on advice from the legal department. However, confusion and frustration on the part of users as well as developments in the litigation context has led to some dissatisfaction with that approach.

Accordingly, it is more typical of current practice for an interdisciplinary team consisting of both functional and user representatives to be assigned to assess an email retention policy. The assessment may be driven by concerns of one of the groups, but it should include representatives of Legal, IT, Records Management (RM), Compliance, Finance, and representatives of major business units – domestic and international. Complex issues are involved when an entity operates both inside and outside the United States because its email system typically encompasses all parts of the enterprise. For example, the entity may decide to adopt decentralized email retention approaches under the umbrella of a single broad policy with individual national policies corresponding to organizational limits – or not. The team is often empowered to assess the current status of the organization's email policy and to make recommendations regarding changes, if any, that may be deemed necessary or desirable, including development of new policy features.

The team should be empowered to call upon and utilize, as appropriate, the expertise of consultants, professional organizations, outside lawyers and vendor representatives. A decision should be made as to what departments or units within the entity are going to be primarily responsible for developing, implementing and monitoring email retention policies for the functions or enterprise as may be applicable to the entity. A fully engaged responsible person should be appointed to lead the team to work closely on implementation, including recommendations on budget or funding decisions as well as monitoring the program after implementation.

Guideline 2: The team should develop a current understanding of email retention polices and practices actually in use within the entity.

Commentary:

It is important for the team to understand the types of email management policies and practices actually in place which may relate to the retention issue. The goal should be to identify the practical gaps, if any, between existing retention policies and actual practices and the costs and risks, including litigation risks, which are present. The results of this analysis can then be useful in discussions of any proposed changes or revisions under consideration.

It will be important for the team to develop an understanding of these basic background questions:

- What are the current policies, processes, work practices, or procedures applicable to the creation, distribution, retention, retrieval, and deletion of email and other electronic communications?

- What contextual information does the email system generate?
- What types of personal or distributed electronic devices are in common usage for handling email?
- What types of content are transmitted or received by email or contained within the message bodies?
- What user management practices are encouraged or tolerated for individual email accounts?
- What access to personal email archives exist on desktop and laptop hard drives and how often they are used?
- What is the role of the user in determining how long email is retained?
- When and how are existing email policies and procedures communicated to users?
- Who (and how many different functions) within the organization is responsible for or has email policies in place?
- How does the organization define a "record" and to what extent (percentage) are emails, usually based on content, included within this definition?
- How are emails with business significance, as defined by records schedules, treated?
- What are the current audit practices and capabilities to assure system integrity?
- Are users required to ascertain and classify email and to what extent is this accomplished?
- How is email integration into records management systems accomplished?
- How are litigation holds applied to email?

Some may find it useful to retain outside consulting assistance to help perform this assessment. Other entities may find it sufficient to conduct their own review of existing policies and interviews, focus groups and surveys, including benchmarking exercises or other informal methods of developing comparative examples of possible policy features.

As a starting point, IT personnel should brief the team on the relevant technology and storage architecture, including all storage locations or potential "sources" of email and attachments. Close attention should be paid to understanding the actual functioning of the active and backup email systems and the policies and practices relating to any backup media which may be utilized.

The team should also be made aware of the relevant legal principles governing the use and retention of email, with some degree of focus on the organization's particular litigation environment. This could include a review of the types of repetitive litigation encountered, the practices followed in preserving accessible and inaccessible sources of information in contemplation of discovery in litigation, and the process followed in identifying and producing email and other information for discovery, together with any costs, burdens, and problems encountered in carrying out the discovery process.

Finally, the records management function should be asked how and whether, if at all, email and attachments are currently expected to be reviewed for content and incorporated into records management storage policies and practices. As noted earlier, the unique regulatory, business and legal requirements applicable to each entity play an important role in determining what reasonable practice is in this regard.

With this input, the team can develop a concise and accurate evaluation of the effectiveness, business needs, costs and risks associated with current practices to help set the stage for an analysis of the need, if any, for revisions in existing policies and practices.

Guideline 3: An entity should select features for updates or revisions of email retention policy with the understanding that a variety of possible approaches reflecting size, complexity and policy priorities are possible.

Commentary:

The selection of appropriate retention strategy for active email in use is the primary focus of any review. In some cases, this review may result in nothing more than establishing supplemental

processes or features to strengthen existing policy, while in others it may involve significant revisions or the development of a completely new strategy. The unique experiences of the entity within the legal, regulatory and business context will govern the types of choices available.

The process of reaching consensus in the face of differing objectives of functional and business representatives is not easy. The team members should be encouraged to openly discuss their differences of viewpoint and identify why they believe them to be important.[15]

Each proposed goal or objective should be assessed in the unique context in which the entity operates. The reality is that the costs and risks associated with change are often a limiting factor and the perceived benefits may not be deemed to be worth the effort and investment required. The risks associated with any particular goal should also be carefully assessed.

Reaching Consensus: The Default Retention Strategy

One place to start is by developing a general consensus on the preferred duration of continued access for users (or groups of users) (the "default retention strategy"). As discussed earlier, there are sharply contrasting practices in existence today regarding the preferred approach.[16]

Some entities focus their strategy on quickly reducing the volume of email that is routinely accessible to users from active sources. The key mantra is that email containing only "transitory" information – of no lasting value – is to be quickly eliminated.[17] This approach requires that careful attention be paid to implementation of the litigation hold process. Any approach that emphasizes short retention of email should also provide alternative local or centralized storage alternatives to enable the retention of information with longer term value ("records").[18]

A contrasting approach is to permit retention of email at the discretion of the user for as long as the user deems it useful (with some outer limits). Here, the argument is that an accurate assessment of the value (needed for "classification") of individual email cannot always be made at the time of generation or receipt of email and attachments.[19] Some also argue that the classification decisions by individual users are, at best, rarely consistent and risk exposing the entity to loss of information needed in the case of litigation. Thus, they assert that the best way to maximize the productivity of users is to allow them to continue to have access to information, regardless of its perceived age or value.

This contrasting approach can be expensive and difficult to implement and has the substantial drawback of increasing the amount of information stored and, therefore, the amount of information which must be searched and reviewed during litigation.

Fine Tuning the Consensus: Choosing Features

After discussing a basic retention strategy and the general objectives related to it, the Team can then seek a consensus on the specific features which will be included in the email policy. To help focus discussion, an attempt should be made to benchmark among similar sized organizations to see what they have found useful, taking into account the strategy they are following.

The process of identifying attractive features and assessing their risks and values should involve the full team and be undertaken in a thorough manner. Consensus will be difficult to reach because all of the viewpoints have validity and should be considered. Naturally, legal and regulatory advice will be crucial, but hopefully the full team will participate.

---

15 *See* Osterman, "E-Mail Archiving Dependent upon Corporate Culture," Network World (March 22, 2005) (describing the resolution of competing views of legal counsel who preferred to purge and a compliance officer who preferred to save email).

16 *See* Ferris Research, "Email Records Management Survey: Guidelines, Technologies, and Trends" (Report 446, September 2004) (26% of respondents require quick deletion).

17 *See, e.g.*, Kahn, "A New Approach to Records Retention," May/June 2006, The Information Management Journal (ARMA) (suggesting that team members should [ultimately] choose between a "get rid of everything immediately" and, "keep everything forever" approach).

18 *See* Tottenham and Brownlee, "Records Management and Best Practices in E-Discovery, Fulbright & Jaworski (2006)(employees drag and drop email with longer term value into networked folders and then automatic deletion can be applied to the user's remaining inbox and sent box items).

19 *See* Priebe and Frankle, "Five Tenets of a Written Document Retention Policy," Securities Litigation, Vol. 18, No. 7 (2004)(copies of most email should be saved since production from central easily-accessible electronic archive will eliminate the need to search individual PCs or backup tapes).

One approach is to ask the team to brainstorm possible features and then rank them in order of importance, taking into account the risks and costs associated with taking or not taking action. An example of how this might be done is shown below:

Choosing Among Alternatives

Specific Features (from a group discussion)	Costs (Tangible or Intangible)	Risks	Forced Rankings
	(Express in dollars)	(Pros and Cons)	

Once adopted, implementing an email retention policy will require careful and focused attention. Typically, the retention policy will be rolled out through targeted training and the use of internal web resources as part of compliance initiatives which will vary depending upon the culture of the entity.

As a supplement to this discussion, we include in the Appendix two alternative forms – at the extremes – of email retention strategies which give some idea of types of features which might be incorporated into a particular policy.[20]

Guideline 4: Any technical solutions should meet the functional requirements identified as part of policy development and should be carefully integrated into existing systems.

Commentary:

A revised email retention policy may require the purchase or licensing of additional software and/or hardware to expand storage capacity, adding new and improved search capabilities or otherwise enhancing the features of existing email systems. All these decisions involve difficult and important technical issues, including the integration with existing systems.[21]

There is no consensus among the Sedona Working Group members on the suitability of any particular software to effectuate retention policy, and this Commentary does not recommend any particular approach. Careful consideration should be taken to ensure that the technology is selected to meet specific goals and that policy and work practices are not being changed solely to match the available technology. The vendors who are offering such products are highly competitive and quite capable of providing targeted suggestions in response to inquires. Any assessment of the suitability of such products should be driven by business, technical and records management considerations, as discussed above, including the potential benefits to users resulting from the presence or absence of features that enhance user flexibility and access.

20 None of the major professional associations, such as ACC, ARMA, AIIM or the ABA have published comprehensive collections of such policies in the private context. The most provocative source of information - thorough benchmarking - must be mined by individual teams on a case by case basis. In contrast, a wealth of examples of public policies and procedures are available for study. *See, e.g.*, "Managing E-Mail," National Electronic Commerce Coordinating Council (2002) (Model Policy for state agencies).

21 *See* Technical Appendix E to Sedona Guidelines (summarizing issues involving the use of electronic (digital) archives, defined as "repositories for electronic records in a form that facilitates searching, reporting, analysis, production, preservation and disposition").

Among the issues that should be examined are:

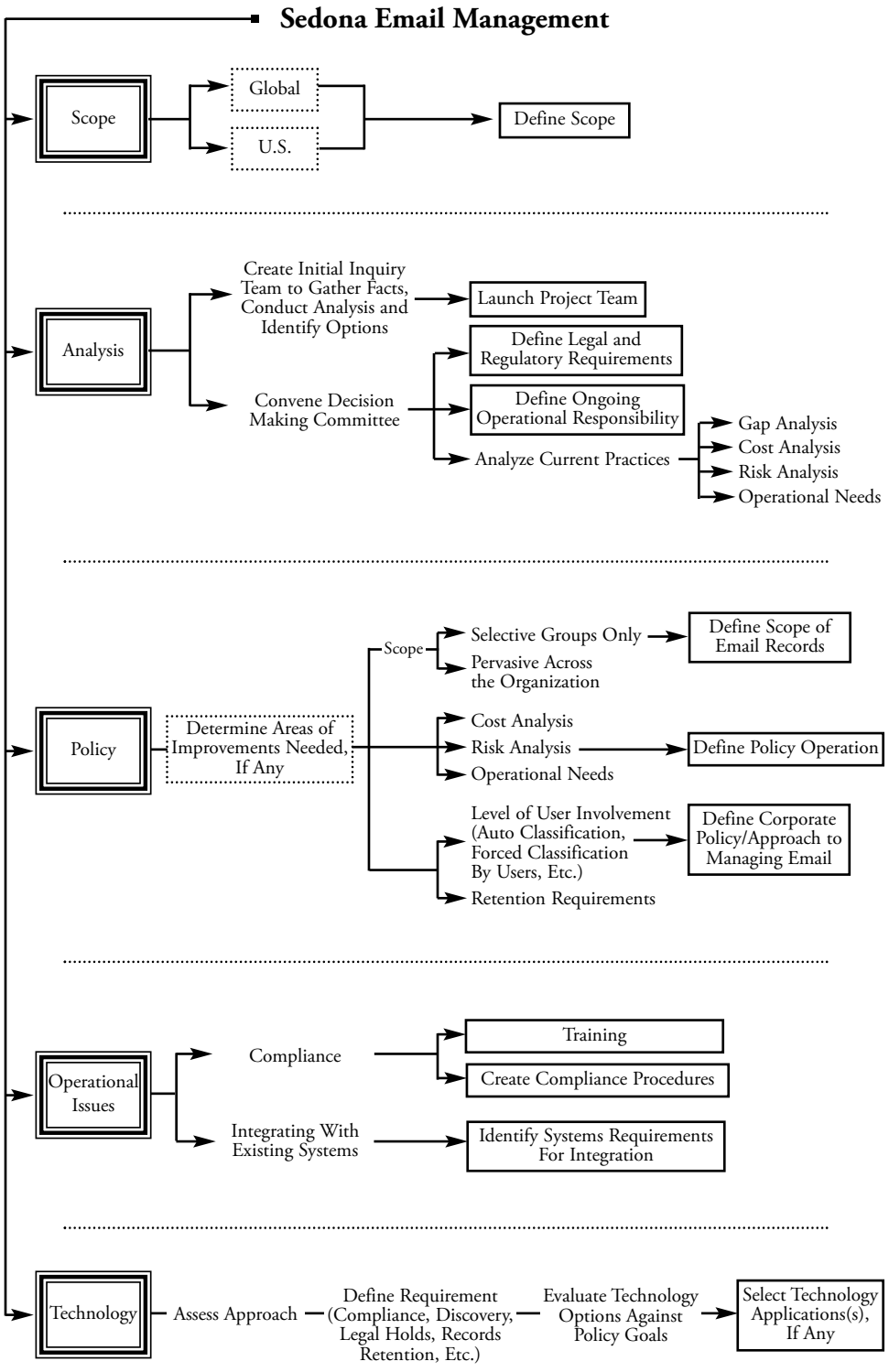
- Ability to be integrated within the entity's technology infrastructure and existing work practices
- Ability to efficiently and accurately search and retrieve information
- Technological assurance, including experience, scalability, performance and ability to integrate with existing systems
- Ability to meet user needs for productive use of electronic information
- Issues involved in migrating from the existing situation
- Costs for the hardware and software – including its acquisition, implementation and ongoing maintenance costs
- Costs associated with user training
- Professional fees needed to implement the solutions
- Ability to identify and retain information with long term records value
- Ability to demonstrate chain of custody, record integrity and respond to metadata concerns
- Ability to integrate with enterprise content management programs
- Ongoing support needs required to fully implement the policy

In the evaluation process, an entity should be aware of the differences between enterprise solutions and so-called "point solutions" – technologies focused on solving a specific problem. There are benefits and drawbacks to either approach.[22] Enterprise-wide solutions can be complex and expensive to implement and risk obsolescence over time.

Perhaps the greatest concern is the tendency to focus on the vendor's view of what are best practices instead of focusing on implementing the entity's policy. Very few vendors have the perspective necessary to tailor their enterprise solutions to an individual entity without careful involvement of the purchaser. Similarly, while targeted solutions can be useful tools in an overall strategy, entities should only make such purchases within the context of an overall enterprise-wide strategy, as it can be difficult to integrate different solutions into existing systems.

Finally, an entity should focus on determining the true cost of adding technology to its enterprise. Some solutions may require additional development to properly customize the system to enable it to be integrated with existing disparate systems. As with any substantial purchase, performing due diligence about the vendor and requesting references can assist in making a well-informed decision.

22 *See* Rugullies and Markham, "Message Archiving Becomes Part of ECM and Storage", Forrester Market Overview (2004)(message archiving decisions should be made in context of storage strategies).


Sedona Email Management
Scope
Global
U.S.
Define Scope
Analysis
Create Initial Inquiry Team to Gather Facts, Conduct Analysis and Identify Options
Launch Project Team
Convene Decision Making Committee
Define Legal and Regulatory Requirements
Define Ongoing Operational Responsibility
Analyze Current Practices
Gap Analysis
Cost Analysis
Risk Analysis
Operational Needs
Policy
Determine Areas of Improvements Needed, If Any
Scope
Selective Groups Only
Pervasive Across the Organization
Define Scope of Email Records
Cost Analysis
Risk Analysis
Operational Needs
Define Policy Operation
Level of User Involvement (Auto Classification, Forced Classification By Users, Etc.)
Define Corporate Policy/Approach to Managing Email
Retention Requirements
Operational Issues
Compliance
Training
Create Compliance Procedures
Integrating With Existing Systems
Identify Systems Requirements For Integration
Technology
Assess Approach
Define Requirement (Compliance, Discovery, Legal Holds, Records Retention, Etc.)
Evaluate Technology Options Against Policy Goals
Select Technology Applications(s), If Any

COMPOSITE SAMPLE POLICY FEATURES

Policy 1.
(Based on short default retention strategy)

- **Core Policy**: Email is retained on an active server only for a short period (e.g., 30 - 90 days), which is enforced by automatic deletion and, perhaps, limits on mailbox size. The user may avoid the deletion only by taking explicit, affirmative actions such as moving the material to dedicated storage on networked files with pre-assigned retention periods. Litigation holds are applied by users to active email and the automatic deletion feature may be suspended by the entity, as appropriate, for key actors for the period until discovery is complete.

- **Related Features**: Users are expected to discard information, store it locally or on networks or print it out in hard copy and incorporate it into existing file structures subject to records management. Roles and responsibilities are clearly articulated for implementation of the policy, including management of litigation holds.

Pros: This approach may help reduce the rate of growth of additional primary server storage. Selected email with longer term value is retained by the user, who is best situated to understand the types of records dealt with on a daily basis and is therefore best equipped to make such classifications accurately and effectively.

Cons: The policy may lead to the loss of information needed by the entity in litigation (for and against the entity's position) because of the difficulty in accurately identifying the importance of particular information within such a short period of time. Users who wish to retain information for longer periods of time may find other methods (such as storing files on a local drive or the use of portable storage media) to retain valued email, thereby making subsequent review during discovery more complex.

Legal Assessment: While some courts are uncomfortable with automatic deletion of active email after a short period, no court has found such a process to be unreasonable where provisions for litigation holds are included and the user has alternative methods of disposition prior to deletion. If discoverable information is not preserved by a user before the copy is eliminated by automatic deletion, but after a preservation obligation has attached, a court will examine whether the use of the automatic deletion feature was "routine" and operated in "good faith," which is fact specific.[23]

Notably, an organization is perfectly free to choose the degree to which it relies upon the discretion of individuals in managing email and applying records schedules; It is not an indication of bad faith to rely upon individual user discretion. That said, an organization must provide those employees with adequate training and direction to exercise judgment with respect to the retention and destruction of emails.

Policy 2:
(Based on indefinite default retention strategy)

- **Core Policy**: Email is retained on active servers for 60 days and then moved automatically to tiered storage and retained indefinitely (or a specified period such as 3 or 5 years). The user is permitted to utilize local archiving or other methods appropriate to his or her work practices. Content management and records management applications are also made available with appropriate search capability for purposes of retrieval for litigation or business use.

23 *See* Fed. Rule Civ. P. 37(f) (effective December 1, 2006) ("Absent exceptional circumstances, a court may not impose sanctions under these rules on a party for failing to provide electronically stored information lost as a result of the routine, good-faith operation of an electronic information system."). *See Turner v. Resort Condominiums International*, No. 1:03-cv-2025-DFH-WTL, 2006 WL 1990379 (S.D. Ind. July 13, 2006)("Rule 37(f) recognizes that discovery should not prevent continued routine operation of computer systems.")

- **Related Features**: The ability to store information on local hard drives may be restricted in order to assure centralized storage of all email. A phased implementation might include archiving of legacy email (as from backup media) introduced as a second step. Roles and responsibilities, including management of litigation holds, may be specified.

Pros: The approach reduces the amount of data stored on the entity's email servers, increases assurance of the entity's ability to access and retrieve information for business or litigation hold purposes, and removes any motivation for users to maintain locally retained information.

Cons: This strategy can significantly increase the amount of stored data that must be searched and reviewed for relevancy, confidentiality, privileges and work product when subject to discovery in litigation. In addition, the costs of installation and maintenance of required systems may be large, and the complexity and reliability of some forms of archiving is still an open issue in some quarters. Finally, entities with a large amount of litigation may find it difficult to find an "open window" in its cycle of repeated litigation holds to effectively dispose of some portion of its ever growing store of email.

Legal Assessment. No court has held that an entity must invest in any particular form of storage technology or otherwise adopt a "save it all" preventative archiving strategy in order to comply fully with common law obligations to preserve potential evidence for pending or anticipated litigation. However, entities that chose some variation of this approach will have an argument that it is not necessary to preserve less accessible sources that may contain relevant e-mails (such as local hard drives and backup tapes) where it is most likely that such sources contain only duplicate information.[24]

24 The Civil Rules Advisory Committee Note to Fed. R. Civ. P. 26(b)(2)(B) explains that "[o]ne factor [that bears on the preservation obligation with respect to inaccessible data] is whether the [responding] party reasonably believes that the information on such sources is likely to be discoverable and not available from reasonably accessible sources." *Accord*: *The Sedona Principles*: *Best Practices Recommendations & Principles for Addressing Electronic Document Production*, Comment 5.b (July 2005 Version) ("Absent specific circumstances, preservation obligations should not extend to disaster recovery backup tapes created in the ordinary course of business. . . . [E]mploying proper preservation procedures with respect to the active system should render preservation of backup tapes on a going-forward basis redundant."); *cf. Zubulake v. UBS Warburg* LLC, 217 F.R.D. 309 ("If unique, relevant information exists on backup tapes, a party may be obligated to preserve and review such tapes.")