The Risk-Cost Retention Model: A New Approach to Records Retention

Bringing all stakeholders to the table to discuss the risk and cost involved in retention decisions allows a company to create the best plan possible for its business needs

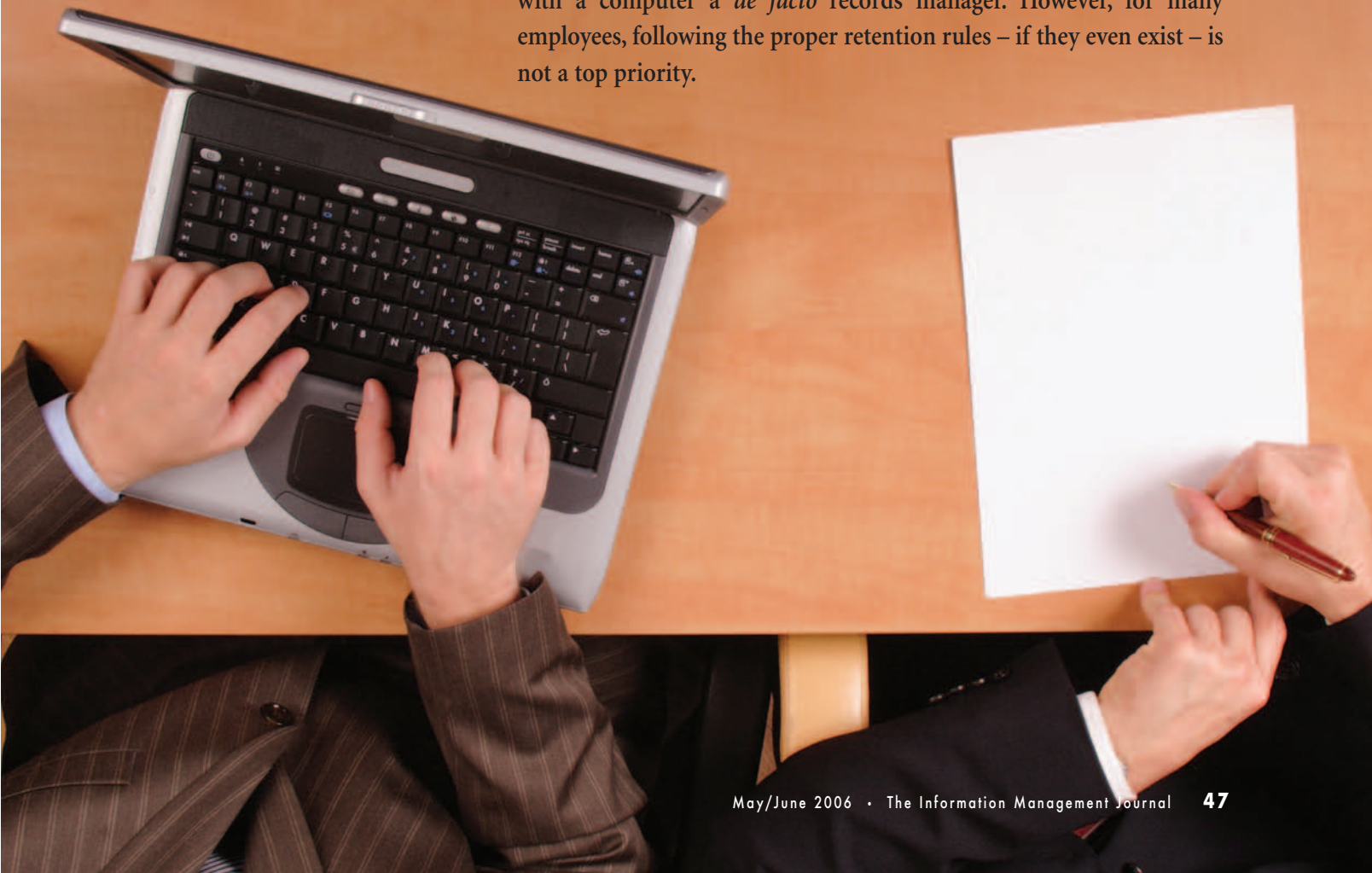
Randolph A. Kahn, Esq.

At the Core

This article

- Reviews the different approaches to retention
- Introduces the risk-cost retention model
- Provides an example of how a business can use the model to determine the best retention plan

Records retention is broken. In the past, this might not have been so serious. But, today records and information management (RIM) matters. Today, the proper application of retention rules to a vast array of business content is more important than ever. Most business information is in electronic form, distributed across more IT infrastructures, facilities, and geographies than ever before. More people – from employees to IT staff members – create, receive, and have control of records, making every employee with a computer a *de facto* records manager. However, for many employees, following the proper retention rules – if they even exist – is not a top priority.



Can You Agree on These Retention Assumptions?

Agreeing with the IT, legal, and business departments on these issues will help organizations determine a functional records retention model.

- Storing information without a business or legal need is not a good use of resources.
- The majority of business records are born digital.
- Laws require retention of some information, including e-records.
- Every organization has some retention responsibility.
- An organization can't keep everything forever.
- An organization can't get rid of everything tomorrow.
- There are business costs and legal risks associated with storage decisions.
- Storage and retention are different activities.
- The volume of records is growing exponentially.

Employees are unlikely to go through each e-mail, spreadsheet, or word processing document, to evaluate, code, and manage it if it requires reviewing a list of hundreds of retention categories to determine the appropriate retention period. If employees are going to get records retention right, it better be fast, easy, and intuitive. The key is to develop a records retention model that is user-friendly, simple, seamless, and easily applied.

Unfortunately, organizations all too often don't have an adequate way to ensure that records are being properly retained. But developing an effective records retention model isn't impossible. Reengineering the development of retention rules can make this task simpler and, therefore, more likely to be successful.

Building an Evaluation Team

Creating a new approach to retention requires input and buy-in from the IT department, the legal department, and business executives, at a minimum. There are numerous interrelated issues that need input from a variety of different perspectives to make sure the new retention plan works for the enterprise overall. Assembling the right team is tantamount to success and to getting buy-in from the rest of the organization.

After assembling the right team, begin evaluating the various retention options for the organization. Gather ideas from colleagues about what may work and develop a list of their suggested approaches. That list may look something like the following one, and even though some of these ideas may not seem feasible – and, in fact, might not typically be considered by the RIM community at all – those tasked with solving the retention problem should expect to find advocates of each of these approaches within their organization.

Some possible retention options:

1. Get rid of everything immediately.
2. Keep everything forever.
3. Set the retention periods by record type for the employees to apply with some RIM help (the traditional approach).
4. Use software to automatically apply retention codes and make decisions about what is a record.
5. Capture a copy of everything on the backup system.
6. Base retention on a fixed period that is long enough to address event-based retention and long retention requirements.
7. Base retention on the business function (i.e., one retention category for everything deemed to be a record in a particular business unit) and provide a way of dealing with exceptions.
8. Base retention on the business function with current retention synthesized into fewer, higher-level categories, organizing them in a way that gives users fewer choices and still makes it legally consistent.

Determining the Best Approach

Getting substantive input from colleagues representing various business units will help build consensus and lead to the best retention solution. For example, lawyers are likely to have different concerns than IT executives, who, in turn, are likely to have different concerns than e-mail server administrators. It is important to determine how the retention option chosen will affect the organization's user needs, business needs, access requirements, legal requirements, and litigation environment. The following risk-cost retention model can be used to help focus the retention discussion on the right set of issues and determine the best approach for the organization.

Using the Model

As a team, discuss for each option

the costs and the risks for each of the issues listed below related to the organization's business, technical, legal, and records management perspectives. Using a scale of 1 to 10, with 1 representing the lowest cost and lowest risk, assign a numeric value to represent the cost and risk in each of the four areas for each of the options listed. Total the numbers. The higher the overall score, the less attractive this approach likely will be for the organization. (See "Risk-Cost Analysis Model Example.")

The model could be customized to add to the analysis other issues (e.g., benefits) or weight to those issues that are of greatest importance (e.g., complying with laws). The focus of this exercise should be to identify the trade-offs that each approach will require.

Discussing the Various Approaches to Retention

Option 1: Get rid of everything immediately.

If an organization got rid of everything shortly after its creation, the cost of management would be low but the risk of not having something that was needed would be high. Risk of system failure would go down because the stuff clogging systems would be purged. There are benefits to this approach, but it may also create risk and legal exposure that are not acceptable. Not being able to produce information for lawsuits or regulators or failing to retain records in conformity with laws would create exposure that well-run organizations will not find acceptable.

Option 2: Retain everything forever.

The risks and costs associated with keeping everything forever may be high. One of the perceived benefits of keeping everything is that it alleviates concerns about not being able to produce something in response to a lawsuit. Yet, when considering the resulting difficulty of finding and retrieving a *specific* item across the enterprise, it is obvious that this could not be done economically and expeditiously. Further, the risk of system failures and costs associated with management would be very high, making this option not as attractive as others.

Option 3: Apply retention by records type with RIM support.

Those representing business units other than records management may be

Risk-Cost Analysis Model

Option	Business Risks & Costs 1=low; 5=medium; 10=high		Technical Risks & Costs 1=low; 5=medium; 10=high		Legal Risks & Costs 1=low; 5=medium; 10=high		RIM Risks & Costs 1=low; 5=medium; 10=high		Total Weight
	Risk to accessibility	Costs of IM & storage	Risk to system functionality or failure	Costs of technology & management	Risk of failing to manage info in conformity with laws	Cost of not being able to produce info in a timely manner	Risk of failing to retain records consistently & in conformity with laws & policy	Costs of information storage when retention is applied	
1. Get rid of everything immediately.									
2. Keep everything forever.									
3. Apply retention period by records type with RIM support.									
4. Use software to automatically apply retention.									
5. Capture a copy of everything on the backup systems.									
6. Base retention on a fixed period of time.									
7. Base retention on business function.									
8. Base retention on business function, synthesizing into fewer higher-level categories.									

concerned that because of the sheer volume of records coupled with the large number and complexity of retention rules, this approach requires too much employee time to code all content correctly. Business executives may see this task as something that they do not want employees spending much time on because they don't view it as adding positively to the bottom line. Another common perception is that employees will always find a way around such processes.

Option 4: Use software to automatically apply retention.

Auto-classification, or artificial intelligence software that can "learn" to get retention right over time, would require virtually no employee's time and may be

Applying the Risk-Cost Retention Model on a Flooded E-mail System

How would the risk-cost retention model work when applied to a real situation? Consider the following example.

Reviewing Background and Attempted "Fixes"

The chief information officer (CIO) of a manufacturing company that employs 10,000 people at locations worldwide is faced with serious e-mail system functionality issues. The company has experienced an exponential growth in the volume of e-mail clogging the company's systems. Growing numbers of electronic discovery requests have taken IT staff away from their real jobs, often for days at a time.

Thus, the CIO imposes several policy "fixes" to address the overburdened e-mail system. First, the CIO cuts mailbox sizes, limiting what employees can store. However, after dealing with minor employee revolts and executives who are not fully on board, the CIO is forced to accept that limiting mailbox size has not really addressed any of the core problems.

So, the IT department issues another directive requiring employees to store e-mail on their local computer in personal folder store (.pst) files or on removable disks rather than on the server. But lawyers intervene, making clear that .pst files only make discovery more burdensome. So, reluctantly, the CIO capitulates.

A new directive is circulated that indicates that the IT department is planning to purge the content of the entire e-mail system every 90 days without regard to its contents. In response to the records manager's concerns expressed to the legal department, a meeting is called by the CIO to develop a better and more holistic approach that deals with the importance of records retention, litigation preservation requirements, and IT systems functionality limitations.

Gathering Input from Stakeholders

A meeting with representatives of various business units with an interest and a stake in decisions surrounding e-mail retention takes place. Following are some of the arguments for various retention approaches that various stakeholders might make in such a situation.

The CIO starts off by saying that the "get rid of everything immediately" approach to retention should be considered. After all, "E-mail is not a record and is not needed" the CIO says, "so don't waste resources any longer than necessary to store 'junk.'"

The records manager is prepared with facts to move the group in a different direction, sharing data about industry use of e-mail for business purposes and concluding by saying that while some e-mails are indeed junk, others are records and must be retained according to the appropriate retention rules.

The company litigation head says that discovery certainly would be made easier and cheaper if there was no e-mail to look through. However, he asserts that as attractive as it may seem, cleaning house of everything tomorrow would violate recordkeeping laws, would likely destroy evidence needed for pending lawsuits, and would in fact destroy information that might be helpful to the company as it tells its side of the story in litigation. Therefore, he advises against such an approach. He reminds the group that the destruction of evidence provisions of the Sarbanes-Oxley Act of 2002 provide decades of prison time for the intentional destruction of certain information in certain situations.

Seeming not to hear the lawyer, the **head e-mail administrator**, who is responsible for e-mail servers, appears gleeful at the prospects that the current server failures and exponential growth in stored messages would be immediately resolved and storage budgets would be freed up to use for other more "productive" IT needs. He makes clear that employees would really appreciate the improved system functionality by getting rid of everything after a short period of time. To himself, he admits that if he advocated this approach to "retention," he might lose a huge part of his storage budget to competing IT projects.

One of the **business unit heads** and a sponsor of the project notes that users would revolt as they "live and die" with e-mail. Therefore, this approach would never be supported by any of the other business executives. He notes that while it would be great not to see so much time and resources wasted, employees could not efficiently do their jobs without records, including e-mail records.

The records manager reminds the group that the company already has a terrific retention schedule that should be applied to e-mail records. However, another member of the team interrupts, noting that employees will not take the time to do retention right if it requires lots of time searching through hundreds of retention schedule choices to find the right code for every e-mail record.

The group goes on to discuss other options but in the end, they

very attractive at first blush. Once coded, record destruction also would be automatic. However, a lawyer may be concerned about allowing technology to code and manage company records knowing that the software will fail a significant percentage of the time. IT may point out that the technology will make fewer mistakes than employees do, but the lawyer will likely point out the difficulty of explaining to a judge why the company records policies are not properly applied a large percentage of the time and why it may have allowed a computer to mistakenly – or illegally – destroy evidence. IT responds that even if the organization doesn't completely rely on such technology, it could be used to help reduce the problem.

just don't know how to come to a conclusion about the right approach to retention.

Applying the Risk-Cost Model and Making a Decision

The group turns to the risk-cost model for help. Collectively the group determines that if all e-mail were destroyed after a short period of time, there would be a great likelihood that needed business information would not be available and concludes that the business risk "Risk to accessibility" of information is extremely high, so the group gives it a "10."

In the next column, the group assesses the cost "Costs of IM and storage" (e.g., people, process, technology) and concludes that if everything was gone tomorrow, it would significantly reduce the costs associated with management and assign it a "1." The group then goes through the remaining technical, legal, and records management risks and costs for this option and the remaining seven options.

The total score column indicates that for this company, keeping everything forever, with 71 points, has the greatest risk and cost so would be the least desirable option. Basing retention on business function, synthesizing retention into fewer higher-level categories scored 24 points and has the lowest risk and cost for this company.

Cost-Risk Analysis Model Example

Option	Business Risks & Costs 1=low; 5=medium; 10=high		Technical Risks & Costs 1=low; 5=medium; 10=high		Legal Risks & Costs 1=low; 5=medium; 10=high		RIM Risks & Costs 1=low; 5=medium; 10=high		Total Weight
	Risk to accessibility	Costs of IM & storage	Risk to system functionality or failure	Costs of technology & management	Risk of failing to manage info in conformity with laws	Cost of not being able to produce info in a timely manner	Risk of failing to retain records consistently & in conformity with laws & policy	Costs of information storage when retention is applied	
1. Get rid of everything immediately.	10	1	1	1	10	10	10	1	44
2. Keep everything forever.	10	10	10	10	1	10	10	10	71
3. Apply retention period by records type with RIM support.	1	10	5	5	1	5	1	5	33
4. Use software to automatically apply retention.	5	5	5	5	10	10	10	5	55
5. Capture a copy of everything on the backup systems.	10	10	5	5	10	10	5	10	65
6. Base retention on a fixed period of time.	5	1	5	5	10	10	10	5	51
7. Base retention on business function.	1	5	1	1	5	5	5	5	28
8. Base retention on business function, synthesizing into fewer higher-level categories.	1	5	5	5	1	1	1	5	24

Option 5: Capture a copy of everything on the backup systems.

Someone from the disaster recovery team may suggest capturing a copy of everything on the backup system and storing it all for a set period of time. This approach brings with it issues of inaccessibility and difficulty in retrieving needed records to respond to business needs, litigation discovery requests, requests from regulators, and other legal requirements. The hard costs of capturing a copy of everything is higher than needed because many non-records also will be saved. Lawyers and records managers may assert that the approach would probably violate the law if records that need to be retained longer are disposed of according to the disaster recovery tape recycle schedule. Records managers would also point out that the disaster recovery system does not provide sufficient RIM functionality.

Option 6: Base retention on a fixed period of time.

Instead of capturing a copy of everything on a backup system, records could be retained wherever located but for a fixed period of time. The discussion around this may be the same as for option 5. In the end, the organization would store a great deal of non-record material without any real benefit. Further, significant costs would be incurred storing and managing this mass of content – particularly when some records would end up being stored and managed on systems that were never designed to deal with the volumes or controls that might be required. Unless the retention was very long, invariably records requiring retention would not be retained in accordance with laws. In addition, such an approach does not provide a satisfactory means to deal with event-based retention of records.

Option 7: Base retention on business function (one retention category for every record in a particular business unit); provide a way to deal with exceptions.

IT might suggest keeping all e-mail for a set period of time based on the business function of the group. For example, accounting would keep everything seven years, human resources would keep everything for 10 years, and so on. While easy, it might be too simple, as it fails to recognize the different kinds of content in each business unit or address records that are subject to event-based retention. In such a situation, the exceptions list would likely be sizable.

Option 8: Base retention on business function, synthesizing retention into fewer higher-level categories that give users fewer, but legally consistent, choices.

This variation may make the most sense to the team. Working together, RIM, IT, and legal staff coalesce categories of records that have the same retention periods and create higher-level "buckets" into which users can drag and drop records. Although it requires more work upfront, it accommodates a number of the issues. It gives responsibility to employees, but having fewer choices makes selection faster and more likely to be done properly.

Keeping Options Open

Using this risk-cost retention model takes a team approach that includes legal, business, IT, and RIM, allows all perspectives and options to be considered, and provides an objective basis for discussing the hard issues around retention and choosing a retention approach that best meets the needs of the organization.

With the proliferation of records – electronic and paper – in today's business environment, it is imperative to choose an approach that makes retention decisions and applications easy for every employee. As the organization's needs change and technology evolves, use the model to consider new or improved approaches with an aim to simplify, simplify, simplify – and then simplify some more.

***Randolph A. Kahn, Esq.**, is the founder of Kahn Consulting, Inc., a consulting firm specializing in the legal, compliance, and policy issues of information management and information technology. He is a two-time recipient of the Britt Literary award, the author of dozens of publications and co-author of* E-mail Rules, Information Nation, Information Nation Warrior, *and* Privacy Nation. *He may be contacted at* rkahn@kahnconsultinginc.com.