

DESIGNING A COMPLIANT RECORD RETENTION POLICY

by

Gregory L. Fordham, CPA, CIA, CCE, Sec+, MCP



WWW.KNFCON.COM

1303 Hightower Trail, Suite 315
Atlanta, GA 30350
800-335-1188

RECORD RETENTION

DESIGNING A COMPLIANT
RECORD RETENTION POLICY

by

Gregory L. Fordham, CPA, CIA, CCE, Sec+, MCP

An organization's record retention policy has historically been focused on meeting two requirements. The first has been management's information requirements. The second has been satisfaction of regulatory record keeping requirements. In many organizations the first of these objectives has been the driving motivation for document retention. In more highly regulated businesses, the latter of these two objectives is likely to be pre-eminent.

In the age of electronic discovery, the design of an organization's record retention policy has increased importance and gained renewed interest. The drivers for this renaissance have been the increased cost of e-discovery, the intolerance to spoliation of digital evidence resulting in numerous decisions imposing sanctions and the extent to which digital evidence has determined the adverse outcome of many a defendant.

When designing a document retention policy for digital evidence, the issues are simple for many. First, there are those who recognize the benefit in having a policy that can destroy evidence of

liability and thus avoid liability.¹ For others it is a means to instruct employees of the correct procedures to follow in order to satisfy their common law requirements and avoid sanctions.

The reality is that neither approach serves the organization well. Indeed, these design objectives are just too simplistic for the many facets that an effective record retention policy must consider. In fact there are many requirements that document retention policy must accomplish. They are satisfaction of:

- Operational and management information requirements,
- Statutory and contractual retention requirements, and
- Disaster recovery.

Each of those general requirements are discussed in the sections that follow.

Operational and Management Information

The period for which records are retained has primarily been driven by how long they are required for operational and management information. In these situations the duration of the record retention typically matches the length of the transaction life cycle. For example

purchasing records are retained for at least 60 days. It takes thirty days to place an order, have the item delivered and then invoiced by the supplier. It then, customarily, takes another 30 days for payment of the goods or services provided. After payment of the item the transaction cycle is closed and the record is typically no longer needed.

Nonetheless, the purchasing transaction life cycle is but one part of the overall business accounting and reporting life cycle that traditionally is measured in annual increments. Thus, although the particular purchasing transaction is completed, it may still need to be retained until the completion of the annual accounting cycle. Until the accounting cycle is closed reference to the purchasing transaction could still be required in case of accounting error or inquiry by the providing vendor.

Even after the annual period is closed, management information is often considered in comparative periods where the current period is compared to the prior period. Thus, the transaction lifecycle for management and operational information is typically at least two years even though any one element could have a much shorter lifecycle.

Statutory and Contractual Requirements

In addition to management and operational information another major reason to retain documents are the requirements imposed by statute as well as contractual requirements. The periods

imposed by statute vary by the types of records and consultation is required to the various imposing statutes.

Contractual requirements are equally as diverse in terms of retention periods. In addition, the event which starts the retention period can be divorced from the event. Consequently, one must have familiarity with the contractual requirements.

The way in which these two operate can have unexpected consequence. On their face, one may appear to have a shorter retention period than the other; but, they can contain trigger features that delay when the clock start for one versus the other such that the apparent shorter retention period ends up having the longest retention period.

For example, a payroll record could have a seven year retention period imposed by statute starting at the time the event occurred. At the same time it could have contractual retention period of five years but the clock does not begin to run until the end of the year in which final payment on the contract was made, which could be years after the event occurred. Similarly, for tax purposes it could have a three year retention period that begins after the filing of the tax return. If the return is filed many years later or never filed then the retention period never begins.

Disaster Recovery

Disaster recovery is not document retention, per se. Rather, disaster recovery is data redundancy.

Data redundancy is different from document retention because it is focused on reconstructing data and not retaining data. In the electronic age, however, many organizations have merged their data redundancy for disaster recovery with document retention. In the process, they have allowed their disaster recovery process to double as the document retention process. They have accomplished this feat by retaining all or at least periodic full backups of their data. As storage costs have become increasingly more economical, it has proven more expensive to analyze and purge redundant or unnecessary data.

An organization's disaster recovery data has drawn considerable attention from litigants. Just as historical disaster recovery data as doubled as archival data, it provides fertile ground for document revisions and a safeharbor against improper document destruction.

In keeping with the desire to reduce the organization's exposure to discovery costs and legal liability, some have advocated limiting disaster recovery processes to only disaster recovery. In the process they shortened backup cycles to days or weeks. This design can be disastrous, however.

The mistake being made about such a disaster recovery plan is that it contemplates only catastrophic events such as fires or other disasters. While a disaster recovery plan serves this

purpose, it must look well beyond a single event occurring in the short term. For example, when designing a disaster recovery plan, would it not also be disastrous if intellectual property had become corrupted and unusable. Would not also be disastrous if when redundant versions of the intellectual property had also been determined to be corrupted and unusable. After all, the corruption could have occurred weeks before. Thus, all of the redundant copies that have been made were of the corrupted data. If the backup cycle is long enough then it will be possible to continue back through earlier and earlier backups until one is found where the data is not corrupted. If the backup cycle is short, however, then the last good version will have been written over by the now corrupted versions. Thus, it is important when designing disaster recovery plans that the backup horizon be longer than the period of time it would take to discover that important data had been deleted or corrupted.

Another failed design plan is the one where all data of a particular class, such as e-mail, is automatically deleted after a certain period of time. The fallacy of this plan is that employees who recognize the need for such data will develop informal data retention mechanisms. Thus, it is better to develop a formal data retention process that emulates reality than to maintain one that is too restrictive and artificially imposed. In such cases the informal system will simply rise and replace the formal system with much less control than if a working formal system had been implemented.

Systems

The systems for managing document retention policies are numerous. In fact they may be as numerous as types of data being managed. Typically, the systems begins with identification of the various document types and matching them to the various retention requirements such as management information, statutory or contractual requirements, or disaster recovery. What becomes difficult is when the various requirements overlap or have complex and nested logic.

With small organizations the rules can be simpler. As the organization grows in size and complexity the rules become much more difficult to manage. In addition, as the number of employees grows just following simple rules can be difficult to achieve consistently.

For smaller organizations a manual or employee based system can be workable. As the organization grows in size and complexity an automated system has appeal. The automated system are known as enterprise content managers. They have risen to prominence as a result of regulatory requirements such as Sarbanes-Oxley as well as document preservation requirements. These have become almost like configuration management systems for all documents from letters, manuals, e-mails to web pages. They often go further than mere retention or control in that they also enable creation, collaboration and publication.

Data Structures

Data structures are the organization given to the data stored under a document retention policy. Typically these structures will recognize the various requirements causing data to be stored.

In the litigation environment the focus has been primarily on e-mail. Thus, if the interest is only e-mail without having to consider other data sources, a solution to retention policy might be easily determined. In such a case, the objective would most likely be the segregation and organization of the e-mail data into smaller sets so that all of the e-mail does not have to be examined.

Such a segmentation of the e-mail store is simple under an e-mail system such as Exchange or Outlook. All that is required is the development of separate databases that corresponds to the storage subject. The subject could be projects for those organizations whose work efforts are project driven or process batches for those that perform processes or even time periods for those whose work is undistinguishable except for the passage of time.

Conclusion

Document retention is a multi-faceted problem that can be made worse by an overly simplistic view to the objective. The problems are typically much more complex and are driven by informational requirements as well as retention and security concerns.

Retention policies that do not appropriately recognize or consider the requirements for document retention or even set retention horizons too short threaten the organization's survivability. After all, the organization may not always be a defendant to a legal proceeding. Even worse would be where critical intellectual property was lost simply because the recovery horizon was too short.

1. *United States v Arthur Andersen, LLP*, 374 F.3d 281, (2004), "There is nothing improper about following a document retention policy when there is no threat of an official investigation, even though one purpose of such a policy may be to withhold documents from unknown, future litigation."