



The Importance of Electronic Record Retention

RFG believes all senior corporate executives, including IT executives, must address the issue of enterprise-wide electronic record retention if they are to satisfy a fundamental element of their fiduciary responsibilities and ensure business continuity. Unfortunately, executives face a growing challenge when managing electronic records, as the amount of electronic knowledge grows exponentially and the formats of electronic data mushroom. In addition, increasing regulatory incursion affects retention requirements. IT executives need to formulate and formalize an enterprise wide strategy to best manage such data now and into the future, so as to reduce the enterprise's legal exposure and ensure future data integrity.

Business Imperatives:

- The existence or non-existence of an electronic record exposes an enterprise to litigation and regulatory non-compliance. In a worst-case scenario, it exposes executive management to investor lawsuits for failure to perform their fiduciary responsibilities. IT executives should check local, state, and national laws regarding electronic record retention, consult with their legal department in the formulation of such a process, and implement a formalized electronic documents retention process company-wide.
 - Employees weeding through electronic inboxes, large file stores, and massive databases are devoting time and energy to ad hoc retention processes. These fall far short of meeting company and government requirements, and waste time and effort that could be better spent benefiting the enterprise. IT executives should define, document, and ensure compliance with a formal archive and retrieval process that also has a rapid recall capability. A side benefit derived by most firms that implement such a policy is the cost savings resulting from the reduction in required storage space.
 - The loss of critical information for business needs can cripple any enterprise. Electronic storage is an important component of an overall records retention practice. IT executives should evaluate business application profiles (BAPs) and user application profiles (UAPs) before vendor investigation, to choose a solution that can meet existing and future enterprise requirements.
-

IT executives are confronted with the growing challenge of managing corporate electronic records. Electronic records can be defined as information created, maintained, or retained in any digitized configuration. Such information can reside on a CD, hard disk, tape, or any other magnetic storage unit. Moreover, record types have expanded from text to audio, fax, music, pictures, video, x-rays, and a variety of other new document and file formats. Records in any or all such formats must be captured, edited, indexed, cross-referenced, retrieved, and eventually erased or destroyed. Faced with this proliferation of information, dispersed amongst various media sources, IT executives

need to formulate a strategy and implement policies to deal with the burgeoning volume of such records.

However, determining what records to keep, where, and for how long are questions that plague many IT executives and employees that are trying to effectively utilize their storage space. There are a number of considerations IT executives have to take into account, such as ease of accessibility, frequency of data use, and legal implications surrounding retention of such data.

There are four areas that IT executives should assess during formulation of electronic record retention policies and procedures. They are, in the order in which they are typically addressed:

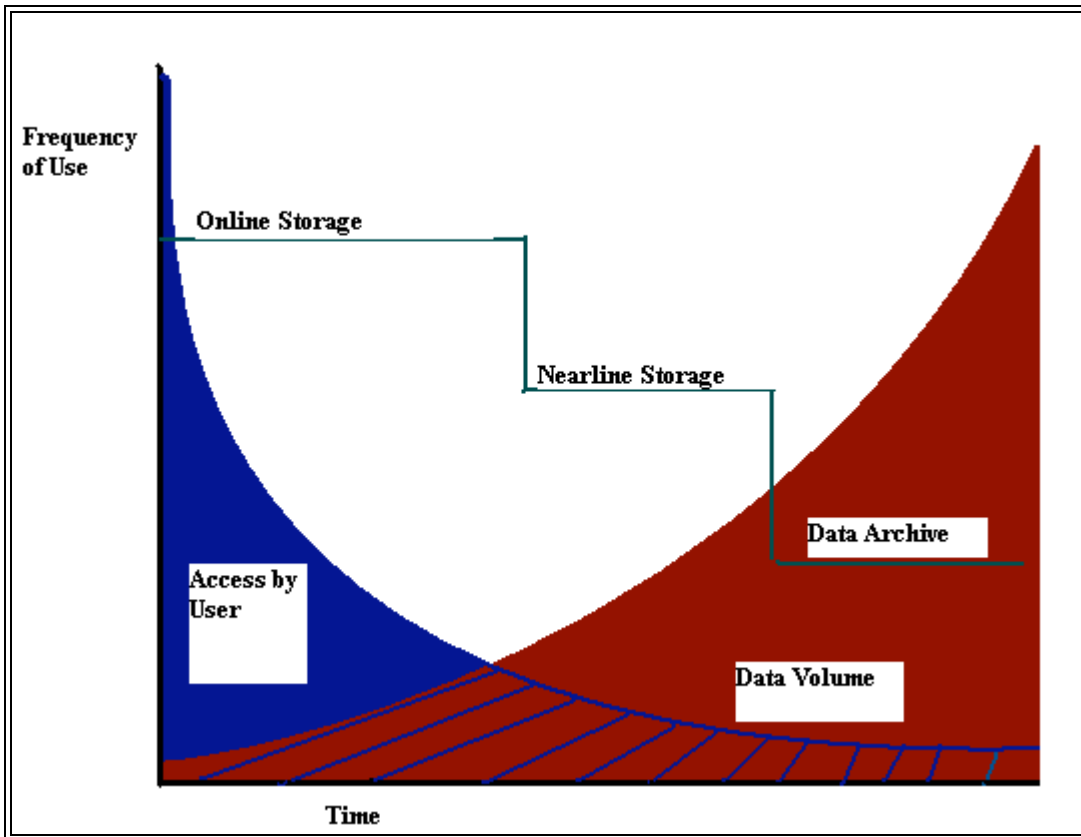
1. the relative business value of the data;
2. current and anticipated legal requirements related to retention of electronic records;
3. the storage infrastructure; and
4. any current policies or procedures already in place.

Electronic Records – Assessing the Value of the Data

There is often confusion regarding which records to keep and in what form. Although each enterprise has different requirements, there are still a few basic guidelines that can be followed to reduce the confusion that often surrounds records retention.

In general, the independent federal agency that oversees the management of all federal records, [The U.S. National Archives and Records Administration \(NARA\)](#) suggests determining the status of a record before determining what should be filed. For example, it is important to determine at what point a draft or working document should be filed. It is also important to create and maintain adequate and proper documentation of the archival process and data catalogue to protect the legal and financial rights of the enterprise, as well as preserve institutional memory. IT executives should consult with line of business (LOB) executives to determine mission criticality of data sets, in order to ensure that data is properly valued.

For most users of desktop systems, an electronic record is created and used in real time. Once such records have been used, are often never again accessed. The figure below illustrates the criticality of data as a function of time.



Source: Robert Frances Group

Such records often reside only on each user's desktop, typically as a document only stored locally, leaving the enterprise vulnerable to loss of critical information. IT executives should look at frequency of records retrieval, and consider it as a major factor when deciding what records to archive. IT executives should then move such records to a near-line, off-line, or archived database. For example, [Storage Technology Corp.](#) suggests that users initially place all data online. Users should then migrate data to "nearline" or "near-online" status after 15 days, and archive or delete data not accessed within 30 days. (See the RFG Research note "[Archiving Critical Corporate Data.](#)")

IT executives should consult with line of business (LOB) executives to formulate a written policy outlining which records will be retained, for what length of time, and in what format or formats. IT executives should also work with LOB executives to establish formal classification categories. For example, data can be classified as critical, sensitive, and non-critical. IT executives will need to determine categories based on their own business requirements. IT executives subsequently file each type according to established guidelines.

Where they exist, IT executives should use BAPs and UAPs to help develop and refine classifications and categories for electronic records. For example, records created with applications related to corporate finances or human resources may have higher retention priority or more stringent requirements than those created with less critical applications.

Similarly, users working with critical records may require more extensive records retention support than those manipulating non-critical or non-regulated business information. At enterprises where BAPs and/or UAPs or their equivalents do not yet exist, record retention policy development efforts could justify creation of such resources. (See the RFG Research Notes "[An Update On The Importance Of Business Application Profiles \(BAPs\)](#)" and [The Importance of User Application Profiles.](#)")

Weighing Legal Requirements – The Sarbanes-Oxley Act

When determining which electronic records to maintain, it is imperative for IT executives to consult with their legal department regarding current and pending legislation pertaining to electronic records management and privacy. This review is necessary for each country in which the company does business. (See the RFG Research Note "[The Challenge of Global Privacy Regulation Differences.](#)")

Numerous regulations exist, and will need to be reviewed to ensure compliance with local, state, and national law. Of recent note for U.S.-based companies is the Sarbanes-Oxley Act of 2002. The act states as its purpose "To protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws, and for other purposes." The act also lays out electronic records retention requirements for all companies regulated by the [U.S. Securities and Exchange Commission](#) (SEC).

Accountants at such companies must now maintain all "audit or review work papers for a period of five years from the end of the fiscal period in which the audit or review was concluded."

The act also states that by the end of 2002, the SEC will issue additional legislation to ensure "the retention of records such as work papers, documents that form the basis of an audit or review, memoranda, correspondence, communications, other documents, and records (including electronic records) which are created, sent, or received in connection with an audit or review and contain conclusions, opinions, analyses, or financial data relating to such an audit or review." Failure to comply carries severe criminal penalties, ranging from fines to imprisonment of upwards of 20 years. IT executives will need to weigh such legal exposure against cost of system implementation; but for most companies strict compliance will be the goal.

Assessing Current Infrastructure

Before undertaking the process of best practices formulation for electronic records retention, IT executives should evaluate the current state of their IT infrastructure. This includes, but is not limited to, hardware, software, and types of records in use (e-mail, instant messages, objects, word processing documents, etc.) This becomes imperative, as IT executives must determine whether or not current resources are sufficient and allocated appropriately in order to ensure the infrastructure's ability to protect critical corporate information.

There are three questions IT executives will need to ask during their evaluation of the IT infrastructure.

1. Can data be managed easily?
2. Can data be replicated as needed?
3. Does current infrastructure allow data to be stored safely and reliably?

IT executives should review all available resources to understand how electronic records are currently provisioned, and what resources exist for their future archival and storage. IT executives should recognize that the same electronic records can exist simultaneously in a variety of media – in CD-ROM, on tape, and on server and client disk drives, for example. IT executives should review current data stores, and eliminate unnecessary duplicate copies to free up storage space, where possible.

There are a number of products available to assist with the archiving, management, and replication of data, and will be explored at a later date. (As an example, see the RFG Research Note "[Princeton Softech – A Corporate Profile](#).") IT executives should begin to investigate the current vendor offerings, in order to determine whether or not a suitable tool exists to help ease the archival process for IT staff. IT executives should also consult with vendors as to planned system upgrades, and future support for new releases of the electronic records management tool. IT executives should attempt to get such promises in writing. (See the RFG Research Note "[Negotiating a Network Service Level Agreement](#).")

Electronic Records: Policies and Procedures

IT executives will need to assess current policies and procedures related to the retention of electronic records. With the evaluation of data importance and infrastructure finished, IT executives should now be poised to formulate a comprehensive strategy to address any gaps in data protection, now and in the future.

During formulation of an electronic records retention strategy, IT executives should consider how records will be accessed and recalled in the future. Part of the records management planning exercise involves longer term planning in addition to the short term. Such a records management process should be a part of a larger business continuity practice. The policies and technologies must be flexible to allow for ongoing changes that are inevitable and that will likely drive retention needs higher. In addition, problems can arise during migration to next-generation hardware or software, or conversion of records to another format. Therefore, IT executives should ensure records retention technologies fit enterprise architecture requirements that are in place to uphold such future growth plans.

IT executives should first assemble a team of LOB executives and IT staff to oversee the initial electronic record retention project. This will help to ensure that the enterprise understands the importance of new procedures and that the importance is communicated throughout various departments. They should develop an agenda for electronic records

retention, taking into consideration prior evaluation of data being generated and current infrastructure. A time frame should be established in which such policies and procedures will be implemented.

The committee should perform a risk assessment, to determine which data sets are most at risk, and how best to address those needs. For example, financial documents may expose the enterprise to more risk if lost than the loss of an internal corporate memo related to a weekly staff meeting. IT executives should also evaluate the economic impact of lost information on the enterprise.

Once a risk assessment is done, plan specifics should be formulated. During this time, IT executives should also negotiate specifics with vendors, train staff, and delegate key decision making responsibilities, to ensure that future questions will be addressed properly. Once plan specifics are in place, they should be tested to ensure enterprise compliance, and should then be modified as needed.

RFG believes that record retention is a critical issue for many enterprises and in its electronic instantiations creates challenges for IT. Once IT executives have all relevant information, they should formulate comprehensive electronic record retention policies, defining which types of documents are to be archived, how they will be archived, and the duration. Only after policy agreement and requirements analysis are in place should new technology evaluation occur. IT executives should consult with LOB executives to assess policies and determine current and future data retention requirements. IT executives should also consult legal counsel to ensure compliance with existing and pending laws regarding the corporate role in the record retention process.

RFG analyst Christie Hangey wrote this Research Note. Interested readers should contact RFG Client Services to arrange further discussion or an interview with Ms. Hangey.

RFG Research Notes provide concise, high-level analysis and recommendations on specific topics of interest to enterprise IT executives. The Notes also provide a framework for further detailed Inquiries by RFG clients, and for follow-up presentations and workshops by RFG research staff available to all interested IT decision-makers. For more information, contact Client Services by telephone at (US) +203/291-6900 or by e-mail at clientservices@rfgonline.com.