ELECTRONIC RECORDS RETENTION:
New Strategies for Data Life Cycle Management

David O. Stephens, CRM, FAI
Roderick C. Wallace, CRM

David O. Stephens, CRM, FAI, CMC
Roderick C. Wallace, CRM

ARMA International
Overland Park, Kansas
Electronic Records Retention: New Strategies for Data Life Cycle Management marks our second effort at defining a practical methodology to enable records and information specialists to apply the principles of records retention to computer-based recordkeeping environments. In 1997, ARMA International published our first work on this subject—Electronic Records Retention: An Introduction. As no such work existed on this subject, we considered writing this book to be something of a groundbreaking endeavor, and we were indeed gratified by the many kind comments we received from our readers. During the past several years, however, many significant occurrences have combined to necessitate the present sequel work. To review these events briefly:

- In 2001, the International Organization for Standardization (ISO) published the first global standard on records management, which endorsed the concept of records retention as a best practice for managing the life cycle of information in all forms and formats.

- In 1997, the U.S. Department of Defense issued its first standard prescribing requirements pertaining to records management software applications; i.e., those designed specifically to manage electronic records. The new standard contains detailed requirements for managing the retention and disposition of such records. Moreover, considerable convergence has occurred between records and document management software solutions, with the integration of functionality for the retention of electronic records as one of the top priorities for these types of software solutions.

- During the mid- to late 1990s, e-mail began to revolutionize the way in which business is conducted. It replaced paper communications and became one of the most business-critical computing applications in any organization—the de facto tool for enterprise-wide communications and collaboration. Many e-mail systems were installed, however, without proper records management and retention methodologies, and e-mail quickly became one of the biggest records management challenges in the U.S. and elsewhere, with significant legal and other risks associated with its mismanagement.

- Also during the mid- to late ’90s, the quantity of electronic records in most organizations (particularly the larger ones) continued to experience very rapid, even explosive, growth. Despite ever increasing capacities in storage media and corresponding decreases in the cost per megabyte, the data storage budgets of many information technology (IT) departments continued to escalate. As a result, data storage management became a top priority for many IT departments that began to recognize the need to control the growth of data and bring better management to storage resources for the first time ever.

- Finally, digital preservation—long-term data retention—became a recognized need in many computing environments during the mid- to late ’90s. Where computerized tax documentation is concerned, in 1998 the U.S. Internal Revenue Service issued Revenue Procedure 98-25, which imposes certain long-term data retention requirements on corporate taxpayers. Moreover, because most if not all of the most strategically important recordkeeping systems in any enterprise now exist solely in electronic form—many having extended retention requirements—organizations are increasingly recognizing the need for new policies and practices to ensure that data will remain processible for as long as it is required.

In short, organizations everywhere are in the midst of a long transition from paper-based to all-digital recordkeeping environments, and they need to employ professional methodologies for life cycle management of computer-based information. Managing computer-based information throughout its life cycle is what this book is about.

As always, we need to thank certain people. First and foremost, we wish to extend our appreciation to ARMA International and specifically to those involved in authorizing the publication of this book. Special thanks are extended to Jean Brown and the Publications Editorial Board, and to Vicki Wiler, Managing Editor.

Our thanks also go to Dr. William Saffady, our colleague and friend, for his contributions to many of the case studies and suggested policies and practices appearing in various chapters of this book. As those who know him will attest, Dr. Saffady epitomizes professionalism in records and information management that is reflected in these pages as in his other professional endeavors. Finally, we extend our most sincere gratitude to our wives and families, without whom this book would not have been possible.

David O. Stephens, CRM, FAI
Smithfield, North Carolina

Roderick C. Wallace, CRM
St. Louis, Missouri
Throughout the world, organizations large and small, public and private, have one thing in common: They create records and information. Electronic Records Retention: New Strategies for Data Life Cycle Management is about what happens to records, specifically records in electronic or digital format, when they cease to be of value to their owners. It is also about how records residing in computer recordkeeping environments are, or should be, systematically destroyed or preserved permanently or for extended periods of time under a formal program, supported by policies, procedures, and technical guidelines that are referred to as records retention.

In traditional recordkeeping environments, when physical records lost their value, they would usually be recycled or simply discarded as office waste. Records having enduring value would be preserved permanently as archival materials. During the past fifty or so years, in cases where records were being managed in accordance with professional principles and practices, the records retention schedule was the principal instrument that governed the life cycle of records. This book addresses the application of these principles and practices to electronic recordkeeping environments. The term we use is electronic records retention, which we define as:

The act of retaining computer-based records in digital storage media for specified, predetermined periods of time commensurate with their value, with subsequent disposal or permanent preservation as a matter of official organizational policy.

Although records retention has been the major strategy for managing the life cycle of records for the past fifty or so years, this methodology has been largely confined to physical recordkeeping environments; it has seldom been employed to manage the life cycle of electronic records. The reasons for this oversight are explored in the next sections.

**RECORDKEEPING AT THE CROSSROADS OF CHANGE**

Throughout the millennia, the records of business enterprises, government agencies, and other organizations have been created in physical format; that is, they resided on visible media—they could be seen and touched, their content could be read and comprehended by sight, without the aid of machines. Visible records have been used throughout recorded history, but recently—only several decades ago—things began to change. With the advent of computers, organizational records began to be created in nonvisible formats.

Some people scoff at the notion of the paperless office or the paperless society; however, when viewed from a long-term perspective, the transition from visible media to all-digital recordkeeping environments is proceeding rapidly and will only accelerate during the ensuing decades. Consider the following:

- According to an article in *Computer Technology Review*, as much as two-thirds of the world’s information is now being “born digital,” meaning that its original occurrence was in a digital format generated by a computer.¹
- According to *The Social Life of Information*, a seminal study by John Seely Brown and Paul Duguid, by the middle of the present century “. . . all information about physical objects, including humans, buildings, processes and organizations, will be online. This is both desirable and inevitable.” [Emphasis added.]²

Furthermore, consider the implications of a study conducted at the University of California at Berkeley:

- The world’s total yearly production of print, film, optical, and magnetic content requires approximately 1.5 billion gigabytes of storage, which equates to about 250 megabytes per person for each man, woman, and child on earth.
- Worldwide, over 7.5 billion office documents are created each year.
- The United States has only about 5 percent of the world’s population, but it creates about 25 percent of all textual information.
- After taking approximately 300,000 years for humans to generate 12 exabytes of information, the next 12 exabytes will be accumulated in just 2.5 years.³

From the foregoing, we conclude that the transition from physical to electronic recordkeeping environments, coupled with breathtaking increases in the growth of electronic records, demands viable solutions for managing the life cycle of these huge quantities of computer-based information. We address in this book what we consider to be the cornerstone of data life cycle management—electronic records retention.
ELECTRONIC RECORDS RETENTION

We have defined electronic records retention as the act of retaining computer-based records in digital storage media for specified, predetermined periods of time commensurate with their value, with subsequent disposal or permanent preservation as a matter of official organizational policy. What, exactly, is required to make records retention a reality in digital recordkeeping environments? Electronic records retention consists of two principal components:

1. **A policy prescribing retention.** This policy must identify the various types of electronic records that exist in the organization and prescribe how long they must be retained. This policy is known as a records retention schedule. This document is a comprehensive list of the various types of records maintained by an organization that indicates the length of time each record type must be maintained as a matter of policy.

2. **Implementation of the retention policy.** At the most fundamental level, every electronic record, every byte of data, will ultimately be subjected to one of two retention actions: It will either be disposed of or preserved permanently. Thus, the implementation of the retention schedule or policy consists of two distinct sets of tasks:
   a. **The disposal of data of temporary value.** For all data having temporary value and is scheduled to be destroyed, practices and tools must be put into place to effect such disposal in a regular and systematic manner. Disposal must occur in two main digital recordkeeping environments: (1) In IT-managed environments. Here, the software supporting all computer applications must have the capability of recognizing expired data and effecting its proper disposal in accordance with the retention policy. The methodology for this process is addressed in Chapters 5 and 12. (2) In user-controlled desktop computing environments. Here, the end-users of all desktop and portable computers must be furnished with guidelines prescribing how to apply the organization’s retention policies for all electronic records under their custody and control. This methodology is discussed in Chapter 6.
   b. **The preservation of data of permanent value.** These data constitute a small but rapidly growing percentage of the total quantity of electronic records of an organization, and nearly all such data reside in computer applications managed by information technology (IT) departments. In cases where data must be preserved in computer-processible format for extended time periods, these departments must implement policies and practices to ensure that such requirements are satisfied. This methodology is addressed in Chapter 11.

The Missing Element in Data Life Cycle Management

As noted previously, records retention has been perhaps the key component of the records management (RM) discipline for almost half a century. This component is based on the simple premise that business records should be retained for as long as they retain value for some business purpose, but no longer. This concept is valid for all business information regardless of its form or the storage media on which it resides. However, the records retention methodology has seldom been extended into computing environments in the United States, at least on a broad scale.

Consider the totality of digital data in your organization or indeed in any given organization and then ask yourself: “What percentage of this mass of data is being retained and disposed of under formal records retention practices?” The answer, in most organizations, will be little or none.

In the computing environments of the U.S., electronic records retention has been largely ignored. The vast majority of electronic recordkeeping systems in the U.S. have been implemented without a predefined methodology for eliminating data, text, and image files at a point in their life cycle at which their information content is of no further value. Moreover, although the vast majority of computer applications contain electronic records that possess temporary value, the few applications that do contain records of permanent value are generally designed with no forethought as to exactly how the permanent retention of digital data can be accomplished. Consequently, electronic records retention is the missing element in the life cycle management of computer-based information.

When Electronic Records Retention Does Not Exist

As stated previously, the life cycle of only a relatively small percentage of electronic records is governed by formal electronic records retention policies and practices. What happens to data in the absence of such policies and practices? In these cases, the data is retained indefinitely. As a practical matter, indefinitely frequently works out to be a period of time roughly, if not exactly equivalent to, the life of the system that supports the data. This practice occurs in cases in which the retention needs for the data are relatively short. Even in cases in which the data needs to be retained for a period of time exceeding the service life of the system that supports it, this requirement is usually handled routinely by IT personnel.

What usually happens is that, when the time comes to upgrade a computer system or application to new technology, the IT personnel who are responsible for managing the system hardware and software will meet with the business managers who “own” the data and ask them whether the legacy data—the existing, older data that remains after the new system has been installed—needs to be migrated to the
When Data Retention Is Not a Problem

As authors, we are unapologetic and vociferous advocates of electronic records retention. In the finest tradition of intellectual honesty, however, we do concede that sometimes data retention is not a problem, and to try to do anything about it would be unnecessary and, perhaps, more trouble than it's worth. Classic records retention theory holds that disposing of records systematically under approved retention policies and practices is always better. However, electronic records retention could be considered to be a solution in search of a problem when the following factors are present:

- When the data needs to be retained for periods of time shorter (or no longer than) the service lives of the hardware and software.
- When the growth of the data is modest and the budget for data storage is stable.
- When the quantity of retained inactive data does not pose a performance problem to the system or a retrieval problem for users.
- When retention of the data is considered to pose little or no legal risk to the organization.

In short, when all these factors are present, when the resources required to implement a data retention solution cannot be justified by the benefits, the organization may feel justified in making a business decision to forego the implementation of formal data retention policies and practices.

A HISTORY OF NEGLECT: WHY?

Why is electronic records retention the forgotten element in the life cycle management of computer-based records? Three fundamental reasons apply:

1. A largely invisible problem. When you walk into an office that is stuffed to the gills with paper files housed in cabinets or open shelving, when you walk into a records center and see the endless rows of shelves and stacks of boxes, the physical manifestations of the records retention problem cannot escape you. As you view these massive stores of records, you can easily and naturally wonder how much of them are useless and should be discarded, if only a good and systematic way to do it were available. Not so with electronic records, which are very compact in size and are not readable by sight. In other words, the phenomenon of useless data is a problem largely without any visible/physical manifestation.

2. Paper vs. electronic records: The double standard. Often when a records manager whose records center has filled up approaches senior management to ask for more money to expand the size of the facility, he/she is likely to be greeted with words to the effect that “Sorry, a lot of that stuff is dead junk. Just throw it away, and then come back to see me and we’ll talk about meeting your needs for more space.” Our point is simply this: In the long history of business computing, senior management never imposed this “common sense” imperative on data processing managers when they budgeted for more and more storage! That type of response just didn’t happen.

3. A solution with no strong advocate. Regrettably, no segment of the computer industry (including its users) has strongly advocated records retention. What is worse, the records management discipline, the group with the strongest professional interest in advocating the concept, failed to come forward with viable retention solutions and attempt to sell them to IT departments or to their users on a wide scale. This neglect continued throughout the first thirty years of business computing. In fact, the first edition of this book published in 1997, marked the first meaningful attempt at proposing a viable methodology for electronic records retention.

To obtain a more in-depth understanding of the history of neglect behind electronic records retention, let's take a closer look at the roles of the various players in the data management story.

Information Technology Departments

Electronic records retention has not been a priority in most information technology (IT) departments because, quite simply, these departments and the individuals who run them have many other issues that usually take precedence over the problem of data retention. The computer industry is, by most accounts, the world’s most dynamic and fast-moving business. Most IT departments must deploy their full resources toward keeping up with this industry and implementing new generations of computer technology throughout an enterprise. As a rule, most IT managers simply have not been able to turn their attention to making sure the data they process is retained...
no longer than is necessary to operate the business. In fact, many IT specialists devote little thought to the data retention issue and often do not even recognize the need for electronic records retention. These perceptions and ways of dealing with them are discussed in Chapter 2.

**Hardware and Software Vendors**

Hardware and software vendors in the computer industry respond primarily to customer/market needs. Because data retention has been such a low priority with most IT personnel, most hardware and software vendors have devoted relatively little emphasis to the issue in their product/systems designs. Most of the industry’s technical talent has been applied to the capture, processing, storage, and retrieval of current, not historical, data. Therefore, hardware and software vendors have devoted considerable attention to data migration—the movement of data from primary to secondary or other storage devices based on life cycle characteristics. However, the disposal or long-term preservation of electronic records has been generally ignored by IT personnel representing their client customers, and therefore it has largely been ignored by the vendor community as well.

Another aspect of the problem is that the need to discard expired data simply never occurs to many IT solution providers. Several years ago, the authors attended the Association for Information and Image Management (AIIM) conference and made the rounds of the vendor exhibits. We asked many vendors whether their system solutions had any functionality for disposing of expired documents or data. Almost without exception, a look of perplexity appeared on the faces of those to whom this question was asked. The common response was along the lines of: “Why would you want to destroy it?” Driven by the mentality that data needs to be processed today, the tomorrow simply never occurs to many IT vendors. This mentality is by no means confined to hardware and software vendors; it is fairly pervasive throughout the IT community.

**Data Owners**

The owners of electronic records are the countless thousands of businesspeople in operating departments who use electronic records every day to conduct business. These users generally have minimal incentives to advocate the disposal of useless electronic records. They are usually content to enjoy machine access to their data for as long as this access can be supported by the IT department. Only rarely do they take the initiative to ensure that data purge functionality has been incorporated into the design criteria of their applications. Even less frequently do they take the initiative to develop and implement electronic records retention on an enterprise-wide basis.

**Records Managers**

As noted earlier, records managers are the information management specialists who have the strongest professional incentives to advocate electronic records retention. The fact that the records management discipline has not made electronic records retention a reality on a wide scale is, we think, one of the profession’s greatest failures. The irony of this situation is that, among all sectors of the information management community, records management is the only professional discipline that offers a viable solution to the problems of uncontrolled growth of records, compliance with recordkeeping laws and regulations, and litigation risk mitigation through systematic document disposal. The solution is records retention. Throughout this book, we discuss how this solution can be applied to electronic records to solve these problems.

**ISO 15489 AND RECORDS RETENTION**

On September 15, 2001, the world of recordkeeping and professional practitioners in the field of records management received the first-ever international standard for records management. On that date, the International Organization for Standardization (ISO), a worldwide federation of national standards bodies based in Geneva, Switzerland, published a document called ISO 15489 and known as the International Standard for Records Management. The document prescribes technical guidelines for recordkeeping in all types of organizational settings, as well as practical guidelines for records managers throughout the world who are responsible for improving the quality of recordkeeping in their organizations.

The issuance of this new global standard marks a milestone in the history of the records management profession. The standard will have the effect of legitimizing records management as a global management discipline; it adds a stamp of legitimacy to records management that it has never enjoyed. Moreover, the new standard provides an officially sanctioned benchmarking model for global emulation of best professional practices.

Section 8.3.6 of the new standard addresses records retention. The standard states:

> Records systems should be capable of facilitating and implementing decisions on the retention and disposition of records. It should be possible for these decisions to be made at any time in the existence of records, including during the design stage of records systems. It should also be possible, where appropriate, for disposition to be activated automatically. Systems should provide audit trails or other methods to track completed disposition actions.

Although this language does not refer specifically to electronic records, the requirements for system functionality implicitly address the issues of electronic records retention. The principles inherent in this new global standard have been incorporated as best practice methodology throughout this book.
A GENERAL POLICY FOR RECORDS RETENTION

The authors’ experience has been that most organizations do not have a policy on records retention.7 Readers may wish to modify the sample policy in Figure 1–1 for their own purposes. The policy is designed to be a general one, providing coverage over the retention and disposal of all records and information—both physical and electronic.

Figure 1–1 Sample Policy

RECORDS RETENTION – GENERAL CORPORATE

SCOPE / COVERAGE: Enterprise-wide, including all departments and other offices or facilities maintaining records and information owned by ABC Corporation.

PURPOSE: The purpose of this policy is to provide requirements and guidelines for managing the life cycle of all company records and information.

POLICY STATEMENT: ABC Corp. hereby declares that it will manage the life cycle of its records and information by developing and implementing a comprehensive Records Retention Program. All company records and information shall be retained and disposed of only in accordance with the retention periods specified in the company’s Records Retention Schedules and with this and related policies and procedures. These schedules are the company’s official policy for information retention and disposal, and they will be developed in accordance with all applicable laws and regulations and good business practices. Compliance with them is mandatory on the part of all departments and employees.

RESPONSIBILITIES:

All Departments and Business Units

All departments and other business units are directly responsible for the management of all records, documents, files, data, and other information pertaining to ABC’s official business in accordance with the law and good records retention principles and practices. To fulfill this responsibility, each department will do the following:

• Appoint a person or persons to serve in the capacity of Coordinator – Records Retention, with overall responsibility for implementing the records retention program within their respective department.

• Implement the Records Retention Schedules for all records and information within the scope of their responsibility.

• Conduct one or more Records Purge Days per year to effect the disposal of all records eligible for such disposition, as provided by the Records Retention Schedules.

Records Retention Coordinators

These individuals are responsible for operating the Records Retention Program within their respective departments or business units. This responsibility includes, but is not limited to, coordinating one or more Records Purge Days each year, initiating any required revisions to the Records Retention Schedule providing coverage for the records of their business unit, and ensuring full and complete implementation of the schedule.

All Company Employees

All employees who create and use records and information are responsible for the following:
• Implementing the Records Retention Schedules on Records Purge Days, and for effecting the daily disposal of E-mail and personal computer-based records and other records as specified herein.

• Ceasing the disposal of relevant records or information promptly upon notification by the Legal Department of a disposal suspension for litigation or other reasons. A disposal suspension means, among other reasons, that the information contained in the records is or may be subject to production under a subpoena or document discovery order issued by proper authority and that disposal under authority of the retention schedules is not authorized.

• Ceasing the disposal of any records or information that may be related to a litigation or a government investigation as soon as either eventuality is reasonably foreseeable, even though a disposal suspension has not yet been formally instituted by the Legal Department. The term “reasonably foreseeable” is defined to mean the point in time at which an ABC employee initially gains knowledge that any particular record or document may or will be relevant to a legal proceeding or government investigation has been or may be instituted against the company. Employees who violate this policy are subject to disciplinary action by the company, up to and including dismissal, and / or judicial penalties imposed by courts of law.

• Ceasing the disposal of relevant records or information promptly upon notification by the Tax Department of a “tax hold” for open tax years. A tax hold means that the information contained in the records is or may be subject to scrutiny by tax authorities, and that disposal under authority of the retention schedules is not authorized.

The Records Management Department

The Records Management Department shall exercise overall management responsibility for the company’s Records Retention Program. To fulfill this responsibility, the Department will do the following:

• Develop and implement a common records retention process throughout the company. The program will consist of records retention schedules specifying the length of time all records and information shall be retained as a matter of policy. The schedules will be based on the company’s legal requirements and business needs, and will include electronic records as well as physical records.

• Develop and maintain a Web site for the Records Retention Schedules on the company’s intranet, together with all policies, practices, and other tools such that all ABC employees can comply fully with the Records Retention Program.

• Develop policies, standards, and guidelines for the operation of facilities for the storage, retrieval, and other management of the company’s inactive records. Assume the direct responsibility for the operation of all facilities for the storage of inactive records throughout the company. All stored records will be adequately protected, managed by computer software throughout their life cycle, and destroyed promptly upon the expiration of their authorized retention periods.

• Review and update the Records Retention Schedules periodically.

Legal Department

The Legal Department is responsible for the following:

• Advising all departments and employees of actual or potential litigation, government
investigations, or other circumstances that will or may result in a suspension of records disposal actions.

- Directing the Records Management Department to issue disposal suspensions formally suspending such records disposal, for specifying the types of records to which these suspensions relate, and for removing these suspensions when appropriate.
- Reviewing the Records Retention Schedules to determine whether they meet the legal needs of the company.
- Providing legal advice to the Records Management Department and to all departments concerning all matters related to the legal aspects of corporate recordkeeping.

Tax Department

The Tax Department is responsible for the following:

- Advising all departments and employees of actual or potential tax audits and the types of records that may be required to support these audits. Also responsible for advising all business units and employees of potential tax controversies and the types of records that may be required to support the company’s position in these matters.
- Placing tax holds formally suspending the disposal of tax documentation for designated tax years, and for removing these holds upon the resolution of all audit exceptions for given tax years so that records disposal may proceed under authority of the Records Retention Schedules.
- Reviewing the Records Retention Schedules to determine whether they meet the tax-compliance requirements of the company.

OTHER RETENTION POLICY GUIDELINES:

Duplicate Copies / Transitory Records

Additional copies of certain records may be maintained by ABC’s employees in their own offices or elsewhere for convenient reference or other purposes. Such additional copies may be in the same format (paper, photographic, or electronic) or in a different format as the record copy. In either case, they are considered duplicate records for retention purposes. They are company property and are subject to this and all corporate records management policies and procedures.

The existence, storage locations, and disposition of duplicate records will not be specifically enumerated in corporate retention schedules. Instead, duplicate records are subject to the following policy:

- Retention requirements for a particular records series are fully and exclusively satisfied by the record copy.
- Duplicate records should be discarded at the earliest practical opportunity when they are no longer needed for reference purposes.
- In no case are duplicate records to be retained longer than the time period stipulated for the record copy.
- The retention of duplicate records is subject to space availability. Duplicate records are not to be sent to off-site storage or microfilmed.

However, some exceptions to these rules should be considered, as follows:

- Employees are cautioned that on some occasions a duplicate record can become a
“new” record and would not, therefore, be subject to these retention rules. For example, when annotations of substantive value are made to a duplicate record, that record then attains value as a separate record, which may need to be considered a new “official” record for purposes of retention.

- Moreover, employees may create copies of certain records series for back-up or vital records protection. Such copies are to be retained in designated storage locations for the same time periods as their corresponding record copies.

Long-Term Data Retention

All retained information must be stored in a manner designed to ensure its accessibility, integrity, confidentiality, authenticity, and legibility. Departments and business units that elect to retain official records in electronic format are responsible for ensuring that the storage media selected for retention purposes (as well as the hardware, software, and other system components) are sufficient to ensure the integrity of the records for the specified retention period. Conversion from one storage medium to another must include adequate controls to support these requirements. (Detailed practices and technical guidelines concerning this matter are contained in the sample policy on long-term data retention in Chapter 11.)

POLICY IMPLEMENTATION:

Intranet / Web-Based Implementation

The company’s prime strategy for records retention implementation shall be to post its Records Retention Schedules on the corporate intranet, together with all the tools necessary to implement them successfully (e.g., policies, practices, litigation / tax hold requirements, etc.). This system of implementation will extend to every desktop in the company, and every employee is required to implement the retention schedules to dispose of records under his / her custody every year.

To ensure full compliance with the retention schedules, every employee must fill out a certificate of retention compliance on the Web site. If an employee fails to complete the certificate, a notice of noncompliance is sent to his / her supervisor, who must take corrective action.

Records Purge Day(s)

NOTES


3 Peter Lyman and Hal R. Varian, How Much Information. (Berkley, CA: University of California, 2000).


6 Ibid., ISO 15489.

The fact that electronic records retention has not been widely practiced in the computing environments of the United States suggests that if electronic records retention is to be done, it must be “sold” to senior IT personnel and other managers and executives. If electronic records retention must be sold, a valid business case must support it—one that is clear and compelling and that makes sense to those who will hear it and approve or reject it. Such a case is presented in this chapter. Further, because nearly every business issue has two sides, including electronic records retention, we present both pro and con arguments and explain the logic behind both. This balanced approach is essential, we believe, for anyone who must stand before senior executives and justify any significant management initiative, including electronic records retention.

This chapter focuses on the benefits of electronic records retention in improving the overall management of stored data in larger enterprises. We consider issues related to the growth of electronic records, the need to control that growth, the costs associated with storing and maintaining electronic records, and how electronic records retention can mitigate those costs. Some very compelling legal reasons support our belief that electronic records retention is in the best interest of organizations. These reasons are discussed in Chapter 3.

THE LOGIC OF THE BUSINESS CASE

Disposing of computer data as soon as it is no longer useful or its retention is no longer required is in the best interest of organizations. This disposition should occur under authority of a formal records retention program. What is the essence of the business case supporting this premise? The logic behind the business case for electronic records retention is summarized by the following questions:

- What is the cost to store and maintain all the computer data in the organization? When building the business case, the total cost of data storage and maintenance must include the cost of administering the data over its entire life cycle, not just the cost of the storage media on which the data resides.
- How much of the current volume of stored data is useless; that is, it is inactive and is no longer needed for any purpose?
- What would be the cost and benefits of disposing of all such data? On the other hand, what will be the costs, risks, and benefits of not doing so?
- What has been the rate of growth in stored data in recent years, and what growth rates are forecast in the foreseeable future? How will this growth affect the overall data storage situation, including the additional costs that must be borne?
- To the extent that data storage is being currently undermanaged or even mismanaged, how could the systematic disposal of useless data contribute to better overall storage management? What costs and benefits would be quantifiable as a result of this disposal?

The answers to these questions constitute the essence of the business case for electronic records retention. They are addressed in the next section.

THE DATA STORAGE AND RETENTION PROBLEM

In many organizations today, data storage management is executed inefficiently, and these inefficiencies can be very costly, particularly for larger enterprises. In fact, according to John Camp, research director of Gartner Inc., savings of at least 20 to 30 percent per year can be realized from a well-implemented enterprise storage management strategy, of which electronic records retention would be one key component. At the bare minimum, any basic storage management strategy should endeavor to embrace the philosophy of minimizing storage resources by retaining the least amount of information required to operate the business.

According to a recent series of articles in InfoWorld on enterprise storage, “at this moment, no aspect of enterprise computing deserves more attention than storing and maintaining corporate data.” The report states that data storage is no longer relegated to the sidelines of IT; in fact, it has been elevated to top priority status in many IT departments. With the capacity of storage devices increasing at 60 percent or more each year and storage prices falling at 35 percent or more per year, this situation creates an environment for a virtually unlimited demand for and consumption of data storage. The end result is the continuing retention of large quantities of unused and probably useless data by most organizations.
In fact, in many organizations, storage management is executed without any real strategy, thus greatly reducing efficiency and cost effectiveness. This practice is certainly true for data life cycle management, implemented through a records retention methodology. For example, a global computer company ran its most important application containing the data that constitutes the very heart of its business in an IBM AS/400 environment, which was installed during the early 1990s. By the late '90s, the size of this business-critical data store had risen to several terabytes. However, never, in the ten-year history of this system, had any useless data been systematically purged, nor were any data retention practices in place. Moreover, this system was being operated with no real data migration functionality in place! The entire data store, including the older inactive data, was being maintained on-line in disk drives. In other words, no consideration had been devoted to the logic of basic records management or retention.

Particularly among larger organizations, the fundamental data storage problem stems from the inability to manage data to keep up with the growth of data. In fact, the trends in computer data storage indicate that less data is being deleted while archival data is being retained longer. However, retaining aged data having very low activity rates on high-performance disks is not economical, a concept apparently ignored by the computer company mentioned previously. Consider the notion that the probability of reuse normally falls to below a few percentage points. According to Fred Moore, a leading authority on computer data storage, "accumulating data indefinitely without implementing retirement or retention policies can turn storage management into waste management." It suggests a compelling argument for why electronic records retention is needed. At a minimum, this situation reflects a poor utilization of system resources. When primary storage devices are overburdened with inactive data, they may not perform at optimum levels. Just as the optimum performance of paper-based recordkeeping systems depends on the regular removal of inactive paper documents from filing cabinets that are then transferred to cartons for off-site storage, so too does the performance of electronic recordkeeping systems depend on a good data migration / records retention strategy.

Chiefly because of the explosive growth of computer data in most organizations, the total cost of data ownership continues to escalate dramatically. Consider, for example, a $10,000 investment in a disk drive. Data storage analysts report that the cost of operating this device is $5 to $7 annually for every dollar spent on the hardware. Thus, the annual cost of operating this $10,000 disk drive would be $50,000 to $70,000. However, the total five-year cost of ownership would approach a quarter of a million dollars! The cost-avoidance strategy of not having to bear the burden of storing and maintaining expired or useless data is more costly in the long run. For every $10,000 in storage hardware costs, a good electronic records retention program can return $50,000 to $70,000 annually!

The obvious way to increase storage capacity is to simply add more hard disk storage. However, the well-known 80:20 rule, whereby 80 percent of the data stored by an organization is hardly ever accessed, means that the costs associated with adding high-performance hard disk capacity is not justifiable in cases where they will be used for storing inactive or even semiactive data. 

### The Benefits of Electronic Records Retention

Having outlined the parameters of the business case for electronic records retention, let’s now "drill deeper" into the benefits of this approach to data life cycle management, in the context of how these initiatives should be sold to senior executives.

Electronic records retention should be proposed to senior IT managers as a “best practice” for data storage management. A recent article in *Storage Management Solutions* defines this best practice as “Archiving data using a centrally managed archival / retrieval system so that end-users and applications benefit from robust records retention services without the overhead of direct management of these activities.” What is needed is a business case based on how electronic records retention can contribute to better overall management of stored data.

### Better Overall Management of Stored Data

Consider the implications of the following statement that appeared in a white paper entitled *The Crisis in Network Data Management*, which was prepared by Epoch, a data storage company:

> More than 80% of the data on any magnetic disk on a typical network has not been touched in 30 days; more than 50% has not been accessed in several months; only 20% of the disk contains active data; and virtually no new space exists for active data.

To the extent that this statement reflects the reality of data management in most network computing environments, it suggests a compelling argument for why electronic records retention is needed. At a minimum, this situation reflects a poor utilization of system resources. When primary storage devices are overburdened with inactive data, they may not perform at optimum levels. Just as the optimum performance of paper-based recordkeeping systems depends on the regular removal of inactive paper documents from filing cabinets that are then transferred to cartons for off-site storage, so too does the performance of electronic recordkeeping systems depend on a good data migration / records retention strategy.

To rectify this mismanaged data storage situation, a combination of an aggressive data migration strategy and an equally aggressive records retention solution is needed. The storage system must be managed so that the primary storage media (the high-performance magnetic disks) are reserved only for the most active on-line data, while semiactive data is relegated to near-line optical media, and inactive data is migrated to magnetic tapes for off-line storage. Finally, the useless electronic records must be systematically purged from the system entirely, under authority of an approved electronic records retention schedule, as soon as their value expires.
Controlling the Growth of Electronic Records

According to Tom Davenport, professor of management information systems at Boston University, “No company I’ve encountered has ever undertaken a major initiative to reduce information overload.” The most basic logic suggests that disposing of useless data, under an established data retention program, would be a key component of any initiative to reduce information overload. Further, such logic suggests that if business records are created in large quantities each business day and are retained indefinitely rather than being systematically destroyed, the organization creating them is experiencing uncontrolled growth of its records. Uncontrolled records growth is certainly the case with electronic records because most organizations lack any effective mechanism to purge expired data from their computing environments at rates even approaching the same rate at which new data are entering their electronic recordkeeping systems.

In view of the absence of widespread records retention solutions, just how out of control is the growth of electronic records in the United States? Published estimates of growth rates for digital data vary considerably. The figures cited most often indicate that traditional “production” applications managed by IT departments exhibit growth rates of 45 to 60 percent per year. However, some Internet, e-commerce applications experience growth rates of 100 percent per year or even greater. The following studies are illustrative of the growth of computer data in the U.S.:

- According to an article in Computer Technology Review, annual storage growth rates are expected to range from 60 percent to over 100 percent annually for the next five years. The average on-line storage requirements of a Global 2000 company in 1998 were 40 terabytes. At the current rate of growth, by 2002 that number will have grown to 300 terabytes.

- The International Data Corporation tracks the total capacity of media shipped and forecasts the growth of data storage. This organization reports that approximately 400 petabytes of storage capacity were shipped in 1997, and they forecast capacity shipments of 3,800 petabytes by 2002.

- An analyst with the META Group forecasts data increases of a hundred fold within the next five years. Moreover, the total expenditures necessary to accommodate this growth will escalate more than ten fold during the next five years. Over the next five years, given a six-fold decrease in price per terabyte and a hundred-fold increase in the quantity of data to be stored, a thirteen-fold increase can be expected in total data management costs.

Although estimates for the growth of stored data vary, regardless of the figure that one accepts as valid, the growth of electronic records today can only be characterized as explosive—unprecedented in all history! The key question, however, is: How has the IT community responded to this explosive proliferation of electronic records? The most common solution: Buy more disk storage space. This “solution” is really no solution at all; it is the equivalent of buying a bigger electronic warehouse each year. However, most IT departments have followed this course of action for decades.

To be fair, the growth of electronic records in most computing environments is so great that no retention solution, however aggressively applied, would result in the disposal of a quantity of digital data equivalent to that which is created every year. For most organizations to dispose of 20 to 60 percent of their electronic records (or whatever quantity would equal the growth of their electronic records) every year seems impractical. However, it would certainly help, and numerous reasons exist for doing so, apart from attempts to stabilize the growth of electronic records.

Reducing Data Storage Costs

A common misconception among many IT specialists is that computer data storage and its attendant costs do not pose a significant problem for an organization because of the sizable increases in media capacity and the corresponding reductions in costs (as expressed in costs per megabyte) for the media. However, this view ignores the overall costs associated with managing data. An estimate of the organization’s total data storage costs (including the cost of administering the storage function) over the entire data life cycle is needed. According to Strategic Research, an information technology research firm, for every $1 per megabyte (MB) spent on disk storage, the total spent in managing that storage ranges from $3 to $8 per megabyte per year. At the larger enterprises, the figure is closer to the top of this range. Other studies put the total cost of managing data storage at three to ten times the cost of the storage hardware and media.

The dramatic rates of growth of stored data has sparked an equally dramatic shift in the role of storage in the management of information technology resources in large organizations. Given the soaring volumes of storage, despite annual decreases in the cost per megabyte, the total cost of managed storage now rivals or exceeds the investment in systems and servers, and often accounts for 50 percent or more of total IT spending. In fact, according to an article in Storage Inc., data storage costs will rise to three-quarters of all IT spending over the next few years.

Part of the problem with arriving at valid estimates concerning the cost-effectiveness of reducing data storage costs through retention solutions is that few total-cost-of-ownership studies are available to provide comparisons of the projected cost of retaining information utilizing alternative media strategies over varying retention periods.

However, let’s take this benefit of reducing data storage costs one step further. If an organization has undefined
retention policies for most or all its applications, the organization is probably retaining far more data than is required to operate its business. How, then, can the benefits of rectifying this situation be quantified? In computing the cost-effectiveness of electronic records retention based on reductions in data storage costs, management must do the following:

1. Estimate the organization’s total storage consumption and its total costs,
2. Estimate the quantity of inactive data that would be subject to being purged under the data retention policy during the first year and in subsequent years (based on projected growth rates), and
3. Calculate the savings resulting from no longer having to store and administer data that is not required to operate the business.

An accurate estimate of the quantity of obsolete or redundant data is difficult to make, but we will hypothetically put the figure at 50 percent—a figure by no means implausible if most or all data are being retained indefinitely. Records managers should work with IT specialists to calculate a valid figure for their organization (and the costs associated with it), and then estimate the savings resulting from the disposal of the obsolete data in year one and in subsequent years. For organizations having a large number of high-volume/high-growth applications that are being retained indefinitely, with a substantial portion of inactive data, the chances are good that an electronic records retention program will pay for itself based solely on reductions in data storage costs, regardless of any other benefits.

In summary, any methodology that can reduce an organization’s total data storage/administrative costs should be highly beneficial in reducing overall computing costs. The business case for electronic records retention should be based on this premise.

BARRIERS AND OBSTACLES: THE OTHER SIDE OF THE BUSINESS CASE

During the past ten or so years, the authors have discussed the merits of electronic records retention with IT personnel from many organizations. Frequently, these individuals proffer various opinions as to why electronic records retention is not needed in their environment. As any salesperson will attest, anyone who attempts to sell anything to anyone had better be prepared for such arguments and be able to address them on their merits. This section addresses these matters.

Electronic Records Retention at the Desktop Level is Impractical

We noted earlier that, with hardware and media prices decreasing at annual rates frequently estimated in the 35 to 40 percent range, the option of not managing storage is frequently considered by some IT managers as the easiest way out.
Hierarchical Storage Management
Obviates the Need

Hierarchical storage management (HSM) is a data storage management strategy in which special HSM software is used to separate active and inactive computer data by migrating files between primary and secondary (and sometimes tertiary) storage media. These data migration routines are based on data access needs, available storage capacity, costs, or other factors. The most active files and applications remain on-line in direct-access storage devices; less frequently accessed data are migrated to near-line optical storage media, or off-line to magnetic tapes. When thus configured, HSM provides a three-tier storage hierarchy for off-line / off-site data backup and archiving. HSM storage solutions have been employed in mainframe computing environments for at least a decade; more recently, new HSM software has been written for network computing environments.

Although HSM is indeed a very powerful data storage management strategy, it does not obviate the need for an electronic records retention program. No software system can make business judgments concerning whether and when to destroy records in an organization's best interest; good records retention policies are needed. Simply migrating the data does not dispose of anything. In mainframe and network computing environments using HSM software, records retention and disposition policies need to be integrated with HSM to produce a total solution to the data retention problem. For a further discussion of HSM and its relevance to electronic records retention see Chapter 5.

Data Warehousing / Mining Software
Obviates the Need

Data warehousing is a computing strategy (effectuated by special software) used to optimize the value of an organization's electronic records on an enterprise-wide basis by assembling records from various applications, platforms, and storage devices into formats for presentation to management for decision-making or other business purposes. Data mining is a similar computing strategy (frequently the terms data warehousing and data mining are used interchangeably by vendors of these technologies).

To better understand the functionality of these data management strategies, consider the following example. A bank may maintain electronic records on specific customers in numerous departments (demand deposits, time deposits, auto loans, student loans, IRAs, etc.). These data are likely to be maintained in several different operating systems or platforms. However, unless they can be assembled from these disparate sources, bank officials cannot assess its overall profitability at the customer level, nor can they make the most informed decisions concerning how best to service individual customers. Data warehousing and/or mining software is designed to make these assessments.

However, as with HSM software, neither data warehousing nor data mining software obviates the need for electronic records retention. Both approaches seek to optimize the value of historical data that may be located in disparate operating environments and platforms, but they do not contain policy statements concerning how long electronic records must be retained, nor do they effectuate any purging of useless data. Thus, they do not replace the need for a comprehensive electronic records retention program.

Records Retention vs. Information
Life Cycle Management

Terminology, can sometimes be of considerable importance in selling a concept within an organizational setting. In the authors' experience, sometimes selling the concept of electronic retention to IT executives under the banner of electronic records retention is difficult. In such cases, what is often needed is a banner utilizing different terminology. We have witnessed a number of instances in which electronic records retention initiatives were successfully sold to IT and other senior executives under the information life cycle banner.

In the past, the term life cycle management has sometimes been used by IT departments in implementing data backup and archiving routines. Electronic records retention, and the incorporation of records retention functionality into electronic recordkeeping environments, may have its best chance of success if it is postured in the context of data life cycle management.

ELECTRONIC RECORDS RETENTION AND THE
FUTURE OF RECORDS MANAGEMENT

In an era when electronic records are exploding in growth, when multiterabyte systems are increasingly common, and when the overall cost of data storage and management is rapidly increasing, electronic records retention is an idea whose time has come.

As the records management discipline makes its transition from visible media to electronic media management, electronic records retention programs must occupy center stage. Indeed, electronic records retention programs for IT departments and for enterprises as a whole must be the top priority of the records management community during the next ten or more years. The remainder of this book presents how electronic records retention can be translated from concept to reality.

NOTES

8 Ibid., “Storage Management Best Practices.”
11 Ibid., “Digital Data’s Future.”
16 “Storage Will Be 75% of All IT Spending Over the Next Couple of Years,” *Storage Inc.*, Quarter 1 2001.
17 Ibid., “Digital Data’s Future.”
18 Ibid., “Migrating Data with HSM.”
19 Ibid., “Migrating Data with HSM,” “Understanding Online Archiving,” and “Enterprise Storage.”
In the previous chapter, we discussed that some very important legal reasons support the need for electronic records retention. Moreover, during the past several years, some important new legislation and regulations have been enacted that have direct and significant relevance for electronic records retention. This chapter addresses these issues.

**REDUCING AN ORGANIZATION’S LEGAL EXPOSURE**

In the opinion of many observers, the opportunity to reduce the risks resulting from liability lawsuits constitutes the most compelling reason to implement electronic records retention initiatives. In fact, in many business environments, these risks are so onerous that an electronic records retention program will be justified based on this benefit alone.

Today, organizations must conduct business in a highly litigious environment; one in which lawsuits are frequently the means of resolving business disputes. In fact, every organization that produces products or services of any kind (or that even hires employees) is faced with threats to its assets as a result of liability lawsuits. These lawsuits are often decided on the basis of old records—records that need not have existed if they had been properly destroyed under an established records retention policy immediately upon expiration of their value for legal and business purposes. When unofficial electronic records are retained through neglect, an organization may possess old, inaccurate, invalid, contradictory, redundant, confidential, even damaging information. As detailed in Chapter 7, the discovery of electronic mail “smoking guns” has grabbed management attention and made headlines in the popular press. Executives have become painfully aware of the risks of having any records available that could be discovered by a potential adversary.¹

Even if the organization has committed no acts that would render it liable under the law, the act of responding to document discovery orders can be very burdensome and expensive. However, these risks and burdens can be greatly mitigated by a well-developed and carefully implemented records retention program. From a litigation risk avoidance perspective, the goal should be to retain only those records needed to conduct business and comply with the law. All other records should be systematically destroyed under a records management program based on records retention periods that are as short as possible.

Retention periods are as short as possible if they reflect the minimum time periods required to operate the business and comply with the law. At the expiration of this period, the records should be systematically destroyed as provided by the retention schedules, assuming that they are not required to be retained by any law or regulation and are not subject to any subpoena requiring their production in a current or pending legal proceeding. If electronic retention periods are constructed based on these precepts, they can go a long way toward mitigating the legal risks that can be associated with the use of computer-based evidence in liability lawsuits.

This problem (and the attendant benefits associated with its resolution) is greatest among businesses that manufacture products subject to failure in performance and/or that may be harmful to the health of consumers or the general public. These types of organizations frequently face significant levels of exposure to product liability lawsuits. Such litigation actions are often decided on the basis of documentary evidence; evidence that comes to the attention of the litigants or the courts during a pretrial procedure known as discovery.

When acts to dispose of electronic records occur in the absence of established policies and procedures, they are inherently arbitrary in nature. From a legal point of view, actions to destroy electronic records are much easier to defend if they have occurred under an approved organizational policy. Why? Because, if the motivation for the disposal should ever become an issue before legal authorities, justifying acts of disposal as having occurred systematically, in the routine course of business, rather than at the whim of employees is easier.

How can an electronic records retention program help to reduce the risks associated with the discovery of evidence in digital form? As indicated previously, by providing for the systematic disposal of electronic records based on retention periods that are as short as possible. Consider this hypothetical example: If an organization no longer retains a certain record and that record is requested as evidence during legal proceedings, the organization must merely justify why that record no longer exists. If, on the other
hand, the record still exists and is requested, it must be produced as evidence and its contents must be defended if they become at issue during the proceedings. The conclusion: An organization’s attorneys can more easily defend the absence of documents that have been systematically destroyed under an established retention policy than they can defend the information content of existing records.

To translate these legal principles into the world of electronic recordkeeping, in the past, lawyers for the plaintiffs seeking incriminating evidence from an organization’s files during the discovery process tended to focus their efforts on evidentiary documentation—paper documents, especially those bearing signatures or other handwritten annotations to the records that could be construed as having high legal value. In recent years, however, litigators have become much more sophisticated about seeking computer-based evidence during the document discovery process. In fact, the evidence gathering process has become so specialized that many litigators now seek to discover electronic records presumed to have been deleted by the user but in fact still reside on storage media because they have not yet been overwritten or erased by the system’s software.

A records retention program for electronic or any other business records must never be used as a shield or justification for illegal or unethical conduct related to records disposal actions. As the case study at the end of this chapter demonstrates, the very purpose of these programs is to enable the organization to demonstrate to legal authorities that all records disposal actions accomplished under the program have been done in good faith and in full compliance with both the letter and spirit of the law. The objective of records retention schedules for either paper or electronic records must never be to exercise “file scrubbing” or “file cleansing” to rid the organization of unfavorable evidence. An adversary in legal proceedings can make a strong case of bad faith in the spoilage of evidence by convincing a jury that a records retention schedule is nothing but a sham for destroying potentially incriminating evidence of negligence or other wrong-doing. Finally, records retention schedules must be systematically developed and applied in the regular course of business. They are not to be applied capriciously or arbitrarily.

ENSURING COMPLIANCE WITH LAWS AND REGULATIONS

In the United States, both the federal and state governments impose numerous laws and regulations requiring regulated parties to retain certain specified records for various periods of time. The process of discovering which regulations apply to a particular type of business and then ensuring that the organization is in full compliance with them can be a very burdensome endeavor. However, the important point here is that without an electronic records retention program supported by thorough legal research to discover these requirements and to ensure that they are reflected in retention periods, an organization has no systematic means of demonstrating compliance with these requirements.

With respect to government-imposed retention requirements applying to electronic records, the most important thing to understand is that government-mandated records retention requirements may apply to electronic records as an authorized or required retention medium. Almost all federal and state laws and regulations that require records to be retained are silent on the issue of which recordkeeping medium may or must be used to satisfy the government’s requirements. Thus, unless a particular storage medium is specified in the law or regulation, regulated parties may feel at liberty to retain the required records on any medium they desire, as long as the records may be reliably produced or reproduced from that medium for the specified retention period.

Government recordkeeping requirements rarely address electronic records per se. As is true with all such generalizations, exceptions exist. Perhaps the most notable exception is Revenue Procedure 98-25, which is promulgated by the United States Internal Revenue Service (IRS). This regulation requires taxpayers maintaining electronic records that contain evidence supporting their tax liability to retain the records for a given tax year, and all software and other related documentation required to process them, until all audit exceptions—disputes between taxpayers and revenue authorities—for that year have been resolved. Because Revenue Procedure 98-25 is perhaps the major electronic recordkeeping regulation applicable to all taxable business entities, its provisions receive more extensive treatment later in this chapter.

Finally, although relatively few laws and regulations pertain to electronic records at present, we are beginning to witness the enactment of many new laws and regulations specifically addressing nonvisible records media. This flurry of legislative activity is expected to continue for at least another ten or so years as lawmakers grapple with vexing questions such as how to demonstrate the integrity of virtual electronic records—those assembled from several sectors of a computing environment, used for a specific business purpose, and then disassembled or “de-created,” with no durable record of their existence, let alone of their content. These issues should remain at the forefront of the records management arena for years to come.

ELECTRONIC RECORDS RETENTION AND RISK MANAGEMENT

Some electronic records retention initiatives are proposed and sold to senior executives in a larger risk management context. According to Deborah Juhnke of Computer Forensics Inc., “the first task in reducing pre-litigation risk is to establish a formal retention and destruction policy and enforce it.” The policy and program that implements it should be based on a needs analysis, a definition of appropriate content, records retention / destruction schedules, and aggressive and rigorously enforced compliance audits.
In a risk management context, the primary goals of electronic records retention are generally enumerated as follows:

1. To create a more efficient and organized recordkeeping system (thereby reducing operating costs);
2. To safeguard and preserve valuable data while eliminating data that is no longer useful or needed; and
3. To reduce potential litigation exposure through proper system management.

As a general rule, the electronic risk management plan should be integrated with the organization’s existing policies on records management. Retention schedules should be defined for all data generated on the organization’s computer systems, including all back-up data. The retention schedules should be integrated with existing document retention policies, making sure that the organization is complying with all legal and document retention periods.

NEW LEGISLATION

During the past several years, some important new laws and regulations that contain direct and significant provisions related to electronic records retention have been enacted. These laws and regulations are reviewed and summarized in the following sections; they appear in full text in the Appendix.

The E-Sign Law

On June 30, 2000, President Clinton signed into law the Electronic Signatures in Global and National Commerce Act, the “E-Sign Act.” This law became effective on October 1, 2000. The electronic records retention provisions of the Act are reviewed next.

The ultimate intent of this new law is to enhance U.S. competitiveness through the widespread use of new technologies. However, in a records management context, the most significant aspect of the new law is that it is designed to remove the barriers and impediments in existing U.S. statutes that have the effect of retarding the development of e-commerce initiatives by businesses. For example, in cases where existing laws require business transactions to be supported by “original records” or documents bearing “authenticated signatures,” the new law is designed to create a legal environment in which to overcome these obstacles by promoting e-commerce initiatives. The Act totally changes the landscape pertaining to the use of electronic information in commercial transactions in the United States. This change includes the retention of electronic records in such transactions.

The law does not, however, grant any special status to electronic records; it merely removes the impediments in existing law to conducting business electronically. In this sense, the law may be characterized as “media neutral.” Electronic records will be subject to the same legal scrutiny as physical records. Nor does the law provide any broad authority or mandate for businesses to convert all types of records from paper to electronic format. The law implicitly recognizes that paper records will be utilized as a medium for business recordkeeping for some time to come.

Records Retention Provisions of E-Sign

The new E-Sign Act contains provisions that pertain directly to electronic records retention in e-commerce environments. These provisions are as follows:

“(d) Retention of Contracts and Records.

(1) Accuracy and accessibility. If a statute, regulation, or other rule of law requires that a contract or other record relating to a transaction in or affecting interstate or foreign commerce be retained, that requirement is met by retaining an electronic record of the information in the contract or other record that:

a. Accurately reflects the information set forth in the contract or other record; and
b. Remains accessible to all persons who are entitled to access by statute, regulation, or rule of law, for the period required by such statute, regulation, or rule of law, in a form that is capable of being accurately reproduced for later reference, whether by transmission, printing, or otherwise.”

Based on these provisions, the law provides three key tests for the legal acceptability of electronic records as a retention medium in e-commerce transactions. These tests are:

- The record must accurately reflect the information contained in the original contract or transaction; and
- The record must remain accessible to those entitled by law to access it, for the period required by law; and
- The record must be capable of being accurately reproduced, whether by printing or otherwise.

If these criteria are not satisfied, the legal validity of the electronic record may be denied. For records and information specialists, the central issue is whether the organization’s e-commerce applications, and the electronic records that comprise them, can be demonstrated to comply with these requirements.

Any computer data supporting e-commerce applications must be retained and destroyed under authority of an officially sanctioned records retention program. All e-commerce data should be scheduled for retention based on retention periods that are sufficient to meet business needs and comply with the law. Such retention periods should be implemented by integrating data purge functionality, consistent with approved retention periods, into the software environment supporting the applications. Records management professionals should work with data owners and IT specialists to ensure that such purge functionality has been properly incorporated into e-commerce applications. Data purge functionality would generally need to be applied at the repository levels for various categories.
of business processes, customer groups, and specific types of transactions.

The Uniform Electronic Transactions Act

The Uniform Electronic Transactions Act (UETA) is a model law adopted by the National Conference of Commissioners on Uniform State Laws on July 1, 1999. The purpose of the UETA is to provide states with a model law that would promote uniformity among state laws addressing electronic records in technology-neutral e-commerce business environments.

Section 12 of the UETA addresses the issue of electronic records retention. It states:

“(a) If a law requires that a record be retained, that requirement is satisfied by retaining an electronic record of the information in the record which:

1. accurately reflects the information set forth in the record after it was first generated in its final form as an electronic record or otherwise; and

2. remains accessible for later reference.”

Section 12 further provides:

“(f) A record retained as an electronic record in accordance with subsection (a) satisfies a law requiring a person to retain a record for evidentiary, audit, or like purposes, unless a law enacted after the effective date of this [Act] specifically prohibits the use of an electronic record for the specified purpose.”

These retention provisions largely mirror those contained in the E-Sign Act. Again, the overall effect will be to promote the widespread adoption of e-commerce technologies and the records that will document the transactions occurring in these types of computing environments.

IRS Revenue Procedure 98-25

Because they apply to electronic records retained by corporate taxpayers throughout the U.S., the electronic records retention requirements promulgated by the Internal Revenue Service are perhaps the most significant federal pronouncements yet made relative to electronic records retention. These requirements are promulgated in Revenue Procedure 98-25, which was first issued in 1991 and subsequently revised in 1998.

The IRS issued these requirements to protect its ability to conduct full and detailed examinations and audits of electronic records providing evidence of tax liability on the part of corporate taxpayers (generally, those with assets of $10 million or greater) during the full period of time the taxpayers maintain records that are subject to scrutiny by revenue authorities. The basic retention requirements are stated as follows: “. . . all machine-sensible data media used for recording, consolidating, and summarizing accounting transactions and records within a taxpayer’s [computer systems] are . . . required to be retained so long as the contents may become material in the administration of any internal revenue law.”

The need for these requirements is similar to the long-term data retention issues discussed in Chapters 10 and 11. For a given tax year, the electronic records of corporate taxpayers can remain open to scrutiny by revenue authorities for extended periods of time; sometimes ten years or longer. “Open” tax years do not become “closed” until all audit exceptions—disputes between the IRS and taxpayers as to the legitimacy of deductions or other issues in dispute—have been resolved. Sometimes these disputes cannot be resolved administratively, and they evolve into litigation that must be disposed of by the tax courts. These matters can take many years.

The problem is that the technology environments in which electronic tax documentation resides may have been upgraded one or even several times before a given tax year is “closed,” which could compromise the integrity of the records and thus adversely impact the ability of the IRS to audit them. Thus, these requirements are intended to ensure that the electronic tax documentation subject to tax audits for any given tax year are retained in fully auditable form for the duration of the taxpayer’s tax liability.

Compliance with Revenue Procedure 98-25 is particularly difficult for companies that acquire other companies and wish to eliminate legacy computer systems of the acquired entities and consolidate them into their own systems. In cases where these legacy systems contain tax documentation, the acquiring entity must ensure that it is in compliance with the requirements of this revenue procedure.

The following is the relevant text from Revenue Procedure 98-25. The full text appears in the Appendix.

SECTION 5. RETAINING MACHINE-SENSIBLE RECORDS

.01 General.

1. The taxpayer must retain machine-sensible records so long as their contents may become material to the administration of the internal revenue laws under § 1.6001-1(e). At a minimum, this materiality continues until the expiration of the period of limitation for assessment, including extensions, for each tax year. In certain situations, records should be kept for a longer period of time. For example, records that pertain to fixed assets, losses incurred under § 832(b)(5) and [*8], LIFO inventories should be kept for longer periods of time.

2. The taxpayer’s machine-sensible records must provide sufficient information to support and verify entries made on the taxpayer’s return and to determine the correct tax liability. The taxpayer’s machine-sensible records will meet this requirement only if they reconcile with the taxpayer’s books and the taxpayer’s return. A taxpayer establishes this reconciliation by demonstrating the relationship (i.e., audit trail);
(a) between the total of the amounts in the taxpayer’s machine-sensible records by account and the account totals in the taxpayer’s books; and

(b) between the total of the amounts in the taxpayer’s machine-sensible records by account and the taxpayer’s return.

(3) The taxpayer must ensure that its machine-sensible records contain sufficient transaction-level detail so that the information and the source documents underlying the machine-sensible records can be identified.

(4) All machine-sensible records required to be retained by this revenue procedure must be made available to the Service upon request and must be capable of being processed.

For a detailed discussion of technical guidelines and best practices for maintaining electronic records in machine-processible format for extended periods of time, see Chapter 11.

The Sarbanes-Oxley Act

During the writing of this book, the U.S. was beset by a number of business scandals that brought to light the need for greater corporate accountability, particularly in matters relating to shareholder accountability and the integrity of the financial and accounting systems of publicly held companies. Perhaps the most infamous of these scandals surrounded the Enron Corporation and Arthur Andersen, which is reviewed at the end of this chapter.

In the wake of these scandals, the United States Congress enacted the Sarbanes-Oxley Act of 2002, which was signed into law by President Bush on July 30, 2002. This new law contains several important provisions pertaining to records retention, including the retention of electronic records. For example, Section 103 requires registered public accounting firms to “prepare and maintain for a period of not less than 7 years, audit workpapers, and other information related to any audit report, in sufficient detail to support the conclusions reached in [the audit report].”

The Act also amends the U.S. obstruction of justice statutes (Chapter 73 of Title 18, United States Code) by placing new, more stringent penalties pertaining to the unlawful destruction of documentary evidence required by federal regulatory bodies for use in investigations or other official proceedings. The new law imposes fines and/or imprisonment of up to 20 years for anyone who knowingly or corruptly “alters, destroys, mutilates, conceals a record, document, or other object, or attempts to do so, with the intent to impair the object’s integrity or availability for use in an official proceeding.”

Finally, the Sarbanes-Oxley Act empowers the Securities and Exchange Commission to promulgate new regulations relating to the retention of records maintained by public accounting firms that serve as documentation of the accuracy and integrity of the financial status of audited companies. These new rules are expected to address matters related to the retention of electronic and paper records of accounting firms and other regulated parties.

CASE STUDY: ENRON AND ARTHUR ANDERSEN

This case study is about a basic principle of law:

When you or the organization for which you work appear about to get into trouble with the law, the law prohibits you or anyone in your organization from destroying any evidence that may be relevant to the issues at hand, particularly documentary evidence that may be construed as incriminating. If you do destroy such records, you could be liable for criminal prosecution and, if convicted, suffer fines or even imprisonment.

Many persons who work for organizations labor under the misapprehension that, unless and until they receive a subpoena, they can destroy documents with impunity. Such a supposition is legally invalid. The significance of this matter can hardly be overstated. Never before in the history of American business has a great global corporation been literally destroyed by acts related directly to document retention and destruction. Yet destruction is precisely what has happened to Arthur Andersen LLP, hitherto one of the world’s pre-eminent public accounting firms.

The Case Unfolds

In early December, 2001, Enron Corporation, a large Houston-based energy company, filed for bankruptcy; one of the largest such actions in U.S. business history. In the weeks that followed, a series of allegations of financial mismanagement, and possible violations of law, began to surface. The affair soon began to spill over to Arthur Andersen, Enron’s outside auditing and accounting firm. Among the allegations were charges that officials of Andersen’s Houston office, who were responsible for managing Enron’s audits, had illegally destroyed documents related to their representation of the company—paper as well as electronic.

On January 15, 2002, Andersen terminated the services of David B. Duncan, the senior partner in charge of the Enron account. Moreover, the following day, Enron terminated the services of the entire firm. A spokesperson for Andersen stated that Mr. Duncan had ordered the destruction of documents shortly after Enron acknowledged that the U.S. Securities and Exchange Commission (SEC) had begun seeking information about Enron financial statements that Andersen had audited. Andersen stated that Mr. Duncan had
Andersen was indicted under a section of the obstruction of a "true bill of indictment" against Arthur Andersen LLP. The indictment stated that "on or about and between October 10, 2001, and November 9, 2001, . . . Andersen, through its partners and others, did knowingly, intentionally and corruptly persuade . . . Andersen employees, with intent to cause and induce such persons to (a) withhold records, documents, and other objects from official proceedings, namely: regulatory and criminal proceedings and investigations, and (b) alter, destroy, mutilate, and conceal objects with intent to impair the objects' integrity and availability for use in such proceedings."17

Section III of the indictment described "the wholesale destruction of documents by Andersen." The indictment stated that, on October 19, 2001, Enron alerted the Andersen audit team that the SEC had begun an inquiry regarding Enron's accounting practices. The indictment went on to state that "After spending Monday, October 22, 2001, at Enron, Andersen partners assigned to the Enron engagement team launched on October 23, 2001, a wholesale destruction of documents at Andersen's offices in Houston . . . Instead of being advised to preserve documentation . . . employees were instructed . . . to destroy immediately documentation relating to Enron, and told to work overtime if necessary to complete the destruction."

**The Indictment: Obstruction of Justice**

The indictment stated that "on or about and between October 10, 2001, and November 9, 2001, . . . Andersen, through its partners and others, did knowingly, intentionally and corruptly persuade . . . Andersen employees, with intent to cause and induce such persons to (a) withhold records, documents, and other objects from official proceedings, namely: regulatory and criminal proceedings and investigations, and (b) alter, destroy, mutilate, and conceal objects with intent to impair the objects' integrity and availability for use in such proceedings."17

The indictment was for a single felony count. If convicted of this charge, the company could receive fines of up to $500,000. What was much worse, Andersen could also lose its license to audit public companies in the United States, which is the major portion of the firm's business. The latter penalty was widely considered to be tantamount to a "corporate death sentence." Thus, this case was about the very survival of the company.

**The Trial**

The trial began in federal court in Houston on May 6, 2002. Space here does not permit a detailed review of the evidence and arguments presented during the twenty-one days of the proceedings. We will, however, present some commentary by Samuel Buell, one of the prosecutors, concerning the document retention aspects of the case. Mr. Buell stated, "There's nothing criminal about having a document retention policy." Characterizing the policy as one that had "gathered dust on the shelf," he said, "What is a crime is to take it out and blow it off and implement it in the middle of an SEC investigation because you want to be able to control what documents the government gets to see and what doc-
THE AFTERMATH: LESSONS LEARNED

As practitioners in information and records management, what can be learned from this debacle? Under what circumstances is the destruction of records an illegal act? How can records and information specialists operate records retention programs to ensure that any and all records disposal actions executed under those programs are lawful? The following points are most relevant:

- First and foremost, records and information specialists must never put themselves in legal jeopardy in exchange for a paycheck from their employers. If you have questions concerning the legality of any records disposal action, contact your Legal Department. If you are still not satisfied, contact the authorities. If the choice is between your company and the law, comply with the law and cooperate with the authorities, even if you must resign your position.

- Under most circumstances in the life of an organization, destroying unneeded records is a perfectly legal act, regardless of whether such disposal occurs under an established records retention program or as just a casual, somewhat arbitrary act of hitting the delete key, overwriting data, or simply discarding records as office waste. In short, businesspeople routinely and lawfully discard unneeded records every business day. The only circumstances under which the disposal of records is an illegal act is when their retention is required by law or regulation or if they are relevant to an actual or pending litigation action or government audit or other official investigation.

- Under the law, destroying documents relevant to an actual or potential lawsuit or government investigation is a crime, punishable by fines and possible imprisonment. This legal prohibition on document destruction begins from the moment at which a person or organization learns of a possible lawsuit or government investigation, even though proceedings have not yet officially commenced.

- Concerning the key question of the point in time at which document destruction becomes an illegal act, the courts have generally applied the “reasonably foreseeable” standard. This standard means that, at the point in time at which litigation or a government investigation becomes a reasonably foreseeable event, the destruction of relevant evidence becomes potentially criminal activity. However, for reasons that were never made clear, this standard was apparently not applied in the judge’s instructions in the Andersen case.

- With respect to the legality of document destruction, the law makes no distinction as to whether documents reside on paper, computer media, or any other format, nor whether they are of “official character” or are merely work papers or duplicate copies rather than “original” records. If the content of any document is or may be deemed relevant to the subject of the lawsuit or investigation, that document may not legally be destroyed and it must be turned over to authorities if requested.

- If records relevant to litigation or a government investigation are requested and cannot be produced, the investigating authorities will demand an explanation. If the records were disposed of, the circumstances surrounding that disposal will be investigated. The investigators will want to know specifically what records were destroyed, what they contained, who destroyed them, when and why. If the motivation behind the disposal was to suppress or conceal unfavorable evidence, those who authorized and/or carried out the disposal could be held liable.

The foregoing requirements of the law supersede any and all organizational policies authorizing document destruction, including the authority granted in records retention schedules. In other words, organizations or any employee thereof cannot attempt to use the authority granted them in records retention policies as justification for destroying information relevant to actual or pending litigation or government investigation; that is, records retention cannot be a shield justifying unlawful disposal of records.

SOME POLICY RECOMMENDATIONS

This entire case and its tragic results could have been avoided if Arthur Andersen had incorporated the following language into its document retention policy and all employees had complied with it fully:
• The Legal Department is responsible for advising all departments and employees of actual or potential litigation, government investigations, or other circumstances that will or may necessitate the preservation of relevant evidence and/or the suspension of related records disposal activities.

• All employees shall immediately cease the disposal of relevant records or information upon notification by the Legal Department of a disposal suspension for litigation or other reasons. A disposal suspension means, among other reasons, that the information contained in the records or may be subject to production under a subpoena or document discovery order issued by proper authority and that disposal under authority of the retention schedules is not authorized.

• Further, all employees shall promptly cease the disposal of any records or information that may be related to a litigation or a government investigation as soon as either eventuality is reasonably foreseeable, even though a disposal suspension has not yet been formally instituted by the Legal Department.

• The term reasonably foreseeable is defined to mean the point in time at which an employee initially gains knowledge that any particular record or document may or will be relevant to a legal proceeding or government investigation, including lawsuits or government investigations that have not officially commenced. Employees who violate this policy are subject to disciplinary action by the company, up to and including dismissal, and/or judicial penalties imposed by courts of law.

If Andersen’s lawyers and employees had only adhered to these principles of lawful recordkeeping conduct, the company would be alive and well today.

NOTES


9 Ibid.

10 This case scenario is an abbreviated version of a longer case study that was published in The Information Management Journal. For more details concerning the evidence presented during the trial (United States vs. Arthur Andersen LLP), see David O. Stephens, “Lessons Learned: The Enron – Arthur Andersen Affair,” The Information Management Journal 36, no. 5 (September/October 2002).

11 For a good account of the events during the early days of the case, see Floyd Norris, “For Andersen and Enron, the Questions Just Keep Coming,” The Wall Street Journal, 16 January 2002.


13 Ibid., “For Andersen and Enron.”


15 18 USCS 1512.


17 Ibid.


20 For an excellent, if somewhat dated, treatise concerning the circumstances under which document disposal can be considered a criminal act, how the prosecutors and the courts administer the obstruction of justice statutes in cases involving document destruction and the relationship of these matters to records retention, see John M. Fedders and Lauryn H. Gutterplan, “Document Retention and Destruction: Practical, Legal, and Ethical Considerations,” The Notre Dame Lawyer 56, no. 1 (October 1980).
This chapter presents ten principles for scheduling electronic records for retention. This chapter is designed to provide a translation of the traditional principles associated with records retention from visible media to electronic recordkeeping environments. These principles are intended to provide records and information specialists with a practical methodology for developing electronic records retention schedules. The authors present a conceptual framework for what electronic records retention is, the principles for developing retention policies for these records, and other information central to an understanding of what is required to implement an electronic records retention program.

**PRINCIPLE NO. 1 – DEFINE ELECTRONIC RECORDS RETENTION**

As noted in Chapter 1, electronic records retention is defined as the act of retaining computer-based records in digital storage media for specified, predetermined periods of time commensurate with their value, with subsequent disposal or permanent preservation as a matter of official organizational policy. To expand on this definition, an electronic records retention program is that component of a larger records management program that provides policies and procedures specifying the length of time that computer-based records must be maintained. An organization’s official policies for electronic records retention are normally expressed in the form of an electronic records retention schedule, with supporting procedures to facilitate its implementation. Finally, this program provides for the systematic destruction of electronic records that no longer serve any useful purpose to the business, as well as the continued retention of digital documents and data that do possess ongoing value for some business purpose.

The methodology for scheduling electronic records is very similar to that employed for visible records media. Records and information specialists must first identify a body of digital information—however large or small—that needs a separate retention period to provide proper instructions to govern its disposition. Then, these specialists, in concert with other professionals, must decide how long the organization needs to retain the records. Finally, records specialists must express the retention periods in a manner that makes implementation practical. Implementation is the essence of electronic records retention. These matters are discussed in detail throughout this book.

**PRINCIPLE NO. 2 – APPLY THE RECORDS SERIES CONCEPT**

In scheduling electronic records for retention, records and information specialists must identify a body of digital information, however large or small, that needs a separate retention period to provide proper instructions to govern its life cycle management. This very important task requires applying the records series concept to electronic records—an essential component in developing good electronic retention schedules.

In scheduling electronic records for retention, a separate retention period must be established for each electronic records series, just as such periods must be developed for each records series residing on visible media. An electronic records series is defined as a separate, discrete body of computer data (text files, data files, or image files) maintained within a computer system, application, or database which is logically related, serves a common purpose or function, and can thus be considered as a separate unit for purposes of developing an electronic records retention schedule. With this definition in mind, let’s now discuss how it should be applied to bodies or groups of data at various levels of a computer application.

Depending on the size and structural complexity of the data, a single computer application may consist of one, several, or many electronic records series, each with separate retention periods, to provide proper instructions to govern the disposition of the data. For some system applications, a single series may cover the entire application, in cases where a single retention period is sufficient to provide for the disposition of all application data. For other applications, several or many records series may need to be defined at the subapplication level; with different retention periods for each series. Rarely will defining electronic records series below the subapplication level—at the data set level—be necessary, as these bodies of data are generally too small to establish a single retention period for each of them.

However, for our purposes here, the key question is: At what level of the system application does a body of computer data exist that needs a separate retention period to govern its disposition? Although assigning retention periods is a judgmental decision that should be made by records specialists in consultation with application developers...
and data owners, usually one or several retention periods for the entire application will be sufficient.

Increasingly, organizations are looking to simplify their retention practices to the maximum extent possible. In this vein, one of the newer trends in retention scheduling is to develop schedules based on relatively broad generic or functional categories. Functional schedules are typically developed at the business process level—one schedule for each major functional area. Moreover, the records categories are defined at the highest, most generic level possible. The result is a much shorter schedule. However, these schedules can sometimes be hard to implement because the users are not furnished with precise guidance concerning the specific records maintained. In order for retention schedules to be effective, they must provide comprehensive coverage and users must be furnished with clear guidance concerning how long all records must be retained. Thus, the level of detail in the schedules must support these objectives.

**PRINCIPLE NO. 3 – USE SOUND METHODOLOGY TO DETERMINE RETENTION PERIODS**

Although a detailed discussion concerning records retention decision making is beyond the scope of this book, the main concepts relating to this process are summarized, as they are so important in developing good retention periods for electronic records. ¹ In short, the retention value of all business information—including electronic records—should be established based on the following five principles:

- **The primacy of content over format concept.** The primary determinant of how long any group of records, including electronic records, should be retained is their content. The format on which electronic information resides is a factor in this decision-making process, but this factor is of secondary importance to the content, the value of that content, and how that value changes over time.

- **The records appraisal concept.** This concept is a familiar one to most records managers, as it has served as the conceptual basis for developing retention schedules for many years. This concept holds that the retention value of business records must be established based on identifying the primary and secondary values of the records, and then making judgments as to when, if ever, these values expire, or decline to the point where disposal of the information can be contemplated. Primary values are those reflecting the basic business purpose(s) served by the records—the reason they were created. Secondary values reflect other uses to which the information may be put during the course of their life cycle—uses that may justify continuing retention after the expiration of primary values. Administrative or operational values are usually identified as primary values, while research or historical values are generally designated as secondary values. Legal value may be either a primary or a secondary value, depending on the purpose and function of a record. A records series can (and usually does) possess several of these values simultaneously, and they may change during the record’s life cycle.

- **The cost / risk / benefit concept.** This concept is no less important in developing good retention schedules for electronic records than the appraisal concept discussed previously. The concept holds that the retention value of any group of records must be established based on the costs, risks, or benefits of retaining the records or disposing of them after varying periods of time. This concept goes further than the records appraisal concept in that it includes consideration of the costs and risks inherent in retaining or disposing of information, not just the values associated with its usage over time. In establishing the retention value of any records series, the records manager should consider the cost to retain it versus the cost savings resulting from its disposal. Moreover, the records manager should determine whether any actual or potential risks are associated with either retention or disposal of the record and, if so, the degree of those risks. Finally, records managers should identify the benefits of retention or disposal and compare them to costs and risks to arrive at a good business decision regarding the retention of the records.

- **The retention options concept.** This concept is simple, but it is often overlooked by records managers in developing records retention periods. It holds that the retention value of any group of records can best be established in identifying options or alternative retention periods, and then making a decision as to the best option. Typically, the retention decision-maker first identifies retention options at the two extremes—the shortest feasible retention period and the longest plausible retention period. At the short extreme, the retention period is so short that its adoption may be uncomfortable for the organization; at the long extreme, the retention period is clearly excessive and will result in the retention of useless information. The best retention periods will often fall somewhere between the two extremes.

Records and information specialists should employ any or all these conceptual approaches when making decisions concerning how long the organization should retain its electronic records. These approaches are designed to bring as much rational thinking as possible to the often vexing question as to how long records should be retained. For some further conceptual guidance relative to the retention decision-making process, retention decision-makers should consider the following four rules:

1. **Avoid the every-conceivable-contingency syndrome.** Records retention periods should not be formulated based on the every-conceivable-contingency syndrome. No records retention program should be designed to accommodate every conceivable need for
information at any future time, no matter how remote the probability of the need might be. In cases where this approach is the basis for retention decision making, excessive retention is sure to be the result. Records specialists must avoid this kind of thinking in formulating any retention periods—electronic or otherwise.

2. **Adopt conservative retention policies where warranted.** Information should be retained if a reasonable probability exists that it will be needed at some future time to support some legitimate business or legal requirement and if the consequences of its absence would be substantial. Where warranted, records retention policies should be conservative in the sense that they do not expose the organization to an inordinate degree of risk. As suggested previously, the goal of the retention program should not be total risk avoidance, but if the only gain from short retention is savings in space, exposing the organization to excessive risk is not justified to attain this reward.

3. **In a litigation-intensive environment, the shorter the better.** Many attorneys believe that old records rarely contain information helpful to the legal defense of an organization. On the contrary, such records can often be misinterpreted and can embarrass an organization or result in more serious legal difficulties. Thus, most attorneys believe that the best way to minimize the legal risks associated with records retention is to provide for their systematic disposal immediately upon expiration of their business value and any legal requirements mandating their retention. Unless litigation or a government investigation has commenced or is foreseeable, destroying records is proper (assuming that all statutory requirements have been satisfied), and doing so will usually be in the organization’s best interest. For a more detailed discussion of this matter, see Chapter 3.

4. **Develop a consensus among responsible parties.** Retention periods are likely to be in the organization’s best interest if they are based on a consensus of opinions from professionals most knowledgeable about the value of the information and the costs, risks, and benefits of its preservation or disposal after various periods of time. Responsible parties would include the officials who currently review and approve the organization’s records retention schedules.

- **The ISO 15489 methodology.** Finally, records and information specialists should consider the guidance concerning retention decision making in ISO 15489, the new international standard for records management. The standard states: “Decisions about how long records should be maintained within a records system are based on an assessment of the regulatory environment, business and accountability requirements and the risk. . . .” Section 4.2.4.3 of the ISO 15489 Technical Report that accompanies this standard prescribes a conceptual methodology for making determinations concerning how long to retain records. The report states: “To determine how long records are maintained, the following five-stage analysis can be undertaken:

  - Determine the legal or administrative requirements for maintaining records within the system.
  - Determine the uses of the record within the system.
  - Determine links to other systems.
  - Consider the broad range of uses of the record.
  - Allocate retention periods to the records on the basis of the total system evaluation.”

If all persons who are involved in the retention decision-making process adhere to the foregoing principles, the organization’s retention decisions should be of top professional quality.

**PRINCIPLE NO. 4 — CONSTRUCT TOTAL LIFE CYCLE RETENTION PERIODS**

If total life cycle control over electronic records is to be achieved, retention periods for electronic records must be constructed to consist of the following components:

- **An on-line retention period.** This period reflects the length of time the data should remain on primary storage devices, usually magnetic disks. This retention will usually be relatively short—a matter of days, weeks, or months; seldom longer than a year or so.

- **A near-line retention period.** This period reflects the length of time the data needs to remain on-site but off-line in secondary storage devices, usually optical media. This retention may also be short—a matter of months or a year or so. However, in some applications it will be much longer.

- **An off-line retention period.** This period reflects the length of time the data needs to remain off-line (and generally off-site), usually on magnetic tapes. Although many organizations without formal electronic records retention programs often retain these electronic records for indefinite periods of time, records managers should apply specific retention periods to them whenever possible.

- **A total retention period.** This period reflects the length of time the data should remain in computer-processible form, after which it should be purged entirely from any and all storage devices supporting the system.

This method of segmenting retention periods for electronic records is particularly relevant in cases where the organization has a hierarchical storage management (HSM) software solution installed. This type of software automates the migration of data from on-line to near-line and off-line storage devices, based on volume, degree of usage, and other criteria. For further details of this type of storage solution and its relevance to electronic records retention, see Chapter 5.
**PRINCIPLE NO. 5 – DETERMINE TOTAL RETENTION PERIODS**

As simple as it sounds, the total retention period for an electronic records series depends on how long the data needs to remain in computer-processible format! If electronic records no longer need to remain in a manipulatable state (that is, the users no longer require computer access to the data), usually no justification for retaining them in a digital, computer-processible format exists. Thus, the total retention period for electronic records would be determined by this requirement.

Legal/regulatory or other business needs may justify further retention beyond the time the electronic version of the records must be retained, but these needs can usually be satisfied by transferring or migrating the data onto an alternative medium for ongoing retention.

**PRINCIPLE NO. 6 – DETERMINE NEED FOR CONSISTENCY IN RETENTION PERIODS**

Consistent retention periods is one of the most controversial and hotly debated issues relating to electronic records retention. In short, the issue is this: In cases where redundant computer data exists on alternate media (e.g., hard-copy printouts, or computer-output microfilm), should the retention period for the electronic versions of the records be longer, shorter, or consistent for all media? Arguments for each of these three points of view are as follows:

- **Retention periods for redundant data should be consistent for all media.** By this logic, if data exists on paper and microfilm as well as on computer storage media, the retention periods should be the same for all formats. The main argument supporting this perspective is that, from a legal point of view, an organization’s retention policies are easier to defend when they are as uniform and consistent as possible. Whether information resides on paper, microfilm, or electronic media does not matter; if the same appraisal criteria are uniformly applied, each of them will be retained for the same length of time.

- **Retention periods for electronic data will / should usually be longer than for data residing on other media.** The main argument supporting this view is that data residing on computer media provides a much greater degree of accessibility for the user than either paper or microfilm; thus, in this sense, the electronic versions are the most valuable. Paper, by contrast, would be considered the least efficient medium; so, the retention period for this format should be the shortest.

- **Retention periods for electronic records will / should usually be shorter than for data residing on other media.** The main argument here is that, by its very nature, computer-based information is valuable because it is highly dynamic; it is processed and manipulated in real time each day in the conduct of current business operations. This characteristic usually has a relatively short life span—usually shorter than paper or microfilm, which are frozen in time and format on more durable media that is more appropriate for longer-term retention needs.

Although each of these arguments has some merit, we believe the best answer is determined by:

1. Defining the organization’s requirements to retain a certain type of information,
2. Determining the access requirements for that information and how they may change during the information life cycle, and
3. Choosing which medium can best meet these requirements during any and all phases of the life cycle.

The retention medium may need to change during the information life cycle, particularly if the retention requirements are lengthy.

**PRINCIPLE NO. 7 – BE HIGHLY SELECTIVE ABOUT ASSIGNING PERMANENT RETENTION PERIODS**

This issue concerns the archival status of electronic records—the capability and appropriateness of digital media for the permanent retention of electronic records of enduring value. Should permanent retention periods be applied to electronic records? If so, under what circumstances should such a decision be made?

The first thing to understand is that computer media used to retain electronic records, and the hardware and software required to read them, do not possess qualities of longevity equivalent to paper and microfilm. If the organization must retain information contained in computer records for many years, paper or microfilm will usually be more practical for meeting its long-term archival needs. Although computer tapes, disks, and other electronic storage media are constantly being improved with respect to their ability to maintain the stability and integrity of their data for long periods of time, these media cannot be read without the proper hardware and software. Because of the rapid obsolescence of computer hardware and software (service lives of less than five years are common), retaining electronic records for long periods of time is usually impractical, even though doing so may be desirable.

However, we do not suggest that records and information specialists should never designate electronic records for permanent retention; rather, they should understand just what such a decision entails and assess the organization’s capability to support this decision over many years. In most computing environments, following the principle of being highly selective about designating electronic records for permanent retention will usually be the proper course of action. This issue of long-term data retention is discussed in detail in Chapters 10 and 11.
Chapter Four: Principles for Electronic Records Retention Scheduling 27

PRINCIPLE NO. 8 – UTILIZE COM OR COLD AS RETENTION MEDIA WHERE APPROPRIATE

For computer records having permanent or long-term retention requirements, records and information specialists should seek to employ retention media that provide properties of stability and durability and are cost-effective and practical to support. In many instances, computer-output microfilm (COM) or computer-output to laser disk (COLD) systems can best satisfy these criteria. These retention solutions should be employed at a point in the life cycle of the records at which they no longer need to remain in a computer-processible format but still require continued retention. The following guidelines are for employing these solutions:

- **Use COLD solutions for medium-length data retention.** COLD systems are often utilized as an archival retention solution for computer-based data. Two principal applications of this technology that are relevant to electronic records retention are as follows:

  1. **COLD as a replacement for on-line storage.** At a point in their life cycle when the data are ready to be migrated from primary storage, they can be downloaded onto optical media, utilized in a COLD system, for near-line or off-line storage. In many computing environments, an organization can realize significant cost savings from using COLD to replace more expensive on-line storage.

  2. **COLD as a COM replacement for medium-term retention.** COLD systems frequently provide an excellent replacement for COM-generated microfiche. Instead of printing the computer reports onto COM, they can be printed onto COLD. These applications are usually very popular because, among other benefits, the archival data can be searched and accessed much more easily on a digital medium such as COLD, as compared to microfilm, a photographic medium. Although the optical media used in COLD applications have good to excellent stability characteristics, this solution is nevertheless vulnerable to technology obsolescence, just as is any configuration of computer hardware and software. Thus, COLD systems should be regarded as providing a medium-term solution for an organization’s data retention needs; these systems should be able to provide reliable retention for time periods ranging from five to ten years.

- **Use COM solutions for long-term data retention.** COM has been utilized as an archival storage solution for the long-term retention of computer data since the 1960s, and it remains a very viable solution for this purpose today. If it has been properly produced and is stored under the proper environmental conditions, COM-generated microfilm can offer excellent archival properties for the long-term or permanent preservation of electronic records. The COM solution should thus be seriously considered for data retention requirements exceeding ten years.

PRINCIPLE NO. 9 – ADDRESS METADATA ISSUES

Metadata is one of the most common, and commonly misunderstood or misapplied, concepts in records management; but it presents one of the biggest challenges related to electronic records retention. Further discussion of metadata is in Chapter 11.

**Meta** is a prefix that means among, along with, or beside. **Data** is derived from the Greek word for information. **Metadata** thus refers to data about data. In information management parlance, the term is used broadly to mean the information about the organization, indexing, classification, and other control devices to manage record objects within a recordkeeping system or records storage environment. Therefore, in a broad context, file folder labels, box labels, and the contents of internal or external indexes would all be considered metadata, as would the control data that accompanies every electronic mail (e-mail) message but is not a part of the message content itself.4

Metadata encompasses all supplementary information in recordkeeping that describes what is in the records, how they are structured, when they were created, why they were created, how they were created and used, who was involved in their creation and use, and where all this activity occurred. Metadata has always been used for organizing, indexing, and retrieving records and information. What is different now is that data and documents increasingly reside in electronic repositories, including the World Wide Web. This change in storage locations raises the importance of metadata to a whole new level. For electronic records, metadata includes some or all of the following:

- A unique record identifier
- Date and time of record creation
- Creator’s organization and identity
- Source of input / identity of originating or native system
- Date and time of modification
- Modifier’s identity and authorization
- Identification of authoritative version
- Media type
- Format
- Location of record
- Addressees / distribution data
- Sensitivity classification5

In scheduling electronic records for retention, consider the following three classes of metadata:

- **Indexing metadata** – That data that provides a logical order with the key record content data needed by the searcher to find the desired information.
- **Records series metadata** – That data that provides logical grouping for records of common application, purpose, and use. Records series data also provides the structural, context, and content components for the grouping.

- **Retention metadata** – That data that provides the location and storage requirements, formats, disposition scheduling, and assorted process data for each records series.

In the context of electronic records retention, metadata is essential for managing record objects throughout their life cycle. The proper management of metadata is essential for preserving the integrity of records objects for as long as they must remain in a computer-processible format. Consequently, the required metadata must support the authenticity of the records objects—their structure and context as well their content—for the full duration of their retention period. Records and information specialists should work with IT specialists to ensure that metadata requirements are properly addressed in all electronic records retention initiatives.

**PRINCIPLE NO. 10 – INTEGRATE RETENTION FUNCTIONALITY WHEN DESIGNING THE SYSTEM**

Whenever possible, incorporating records retention functionality into the design of electronic recordkeeping systems at the time of initial system design is always desirable; that is, prior to system implementation. Otherwise, such functionality must be retrofitted at some later time. The term *retention functionality* has two meanings:

1. For data of temporary value, the software has been designed with the capability to recognize expired data that is eligible for destruction and effect such destruction as per the retention periods at the outset of the system. See Chapter 12 for details.
2. For data requiring permanent retention, the several best practices required to support such retention have been addressed at the outset of system design. See Chapter 11 for details.

These principles are embodied in ISO 15489, which states that “…In electronic records systems, the determinations about capture and retention should be considered in system design at the outset.”

Records and information specialists should work with applications developers and other IT personnel to ensure that the requisite functionality to implement any and all retention periods governing the disposition of electronic records has been incorporated at the time of initial system design.

**NOTES**

As discussed in Chapter 1, enterprise electronic records retention initiatives must be implemented in two main digital recordkeeping environments: (1) in IT-managed environments; and (2) in user-controlled desktop computing environments. This chapter addresses the first of these initiatives; desktop data is the subject of Chapter 6. Our focus here is to prescribe a methodology for scheduling production applications for retention. For our purposes, production applications are defined as those computer system applications that contain business records that need to be scheduled for retention; that is, they are of official character and operational importance and their life cycle needs to be governed by formal records retention policies and practices. These applications are normally managed by IT departments, mostly in the larger mainframe and client/server computing environments.

Unlike the unstructured documents and data residing in desktop environments, production applications contain data that tend to be highly organized and structured and subject to the relatively rigid management controls imposed by IT departments. As noted in Chapter 1, however, the life cycle of the data in these applications is rarely managed by formal electronic records retention policies and practices. Thus, in this chapter we propose a practical methodology for managing the data life cycle; one that any records and information specialist can use in working with IT specialists, owners and users of application data, and other interested persons to develop electronic records retention policies and practices for effective data life cycle management.

**WORKING WITH INFORMATION TECHNOLOGY (IT) SPECIALISTS**

The following principle associated with electronic records retention is true in all computing environments, but it is especially true in larger computing environments:

*Records management specialists will find that undertaking successful enterprise initiatives in electronic records retention is impossible (and certainly undesirable) without working closely with IT personnel.*

Although less true today, historically a certain degree of antipathy has existed between the records management and IT disciplines. Traditional political structures, budget rivalry, and organizational hubris may have contributed to this somewhat strained relationship. Where this regrettable situation exists, records specialists need to be proactive and take the first steps, go the extra mile to overcome any past difficulties and build bridges of rapport with the IT community. The reality is that IT managers and applications developers will probably not attempt to learn to speak and do records management on their own. Therefore, the onus is on records specialists to develop an acquaintance with information technology terminology, environments, and issues.

However, the situation is much improved over what it was during the ’80s and ’90s. Indeed, nearly everywhere we go these days we find records and IT specialists engaged in excellent working relationships to solve retention and many other records management problems. In this age of digital recordkeeping, these cooperative relationships are absolutely essential in order to achieve success in any significant enterprise initiative in records management or retention.

**SKILL SETS REQUIRED**

Some records management specialists lack the requisite experience to work with IT personnel. What skill sets are required to work effectively with IT personnel on electronic records retention initiatives? What skill sets are required in order to develop and implement effective retention and life cycle management policies and practices for electronic records? We consider the following skill sets to be essential:

- General knowledge of mainframe, client / server, and PC-computing environments and the hardware, software, and other resources that run the applications in them.
- General knowledge of computer system applications and the structure of the data that reside in them; specifically, an understanding of standard business processes and data flows.
- Good substantive knowledge of the traditional principles of records inventorying and retention schedule development, including methods of data gathering, legal research, records appraisal, and retention decision making.
- Good substantive knowledge of electronic records retention, as discussed in this book and in other published literature.
Any records specialist who possesses good skills in these areas should be able to do enterprise electronic records retention projects. Although computer programming skills can be useful, they are certainly not required for scheduling electronic records. However, a good working knowledge of basic computer terminology (see the Glossary), issues, trends, hardware, software, and processes is definitely necessary to perform effectively in electronic records scheduling projects.

For anyone with scant background or experience with IT issues, the prospect of such an alien environment can prove daunting. Educational resources are available; e.g., in-house training, formal courses at local educational institutions, vendor seminars, association conferences (ARMA, AIIM), textbooks, trade books, magazines, and journals. These sources can bring one’s level of awareness to the point needed for working successfully with IT personnel on electronic records retention initiatives.

**ELECTRONIC RECORDS RETENTION AND THE INFORMATION TECHNOLOGY (IT) ENVIRONMENT**

Although a detailed discussion of business computing and IT environments is beyond the scope of this book, we focus some attention on several issues that are directly relevant to electronic records retention.

**Computer Data Storage**

As discussed in Chapter 2, from an IT perspective, electronic records retention initiatives are viewed as an approach to improve the management of stored data. Thus, a basic understanding of relevant data storage issues is necessary to schedule IT-managed system applications for retention.1

Data storage devices can be categorized in terms of their storage capacity and speed of access. Generally, at the top of the storage hierarchy tree is computer memory (expensive, fast), followed by hard disk drives, optical storage, and then magnetic tapes. At the bottom is off-line media and perhaps also microfilm, both relatively inexpensive but requiring lengthy access times. The following common computer data storage methodologies are employed by IT departments in larger computing environments:

- **Server-hosted storage**—This type of storage remains the most popular storage solution, at least in the client / server arena. Despite its popularity, however, this solution suffers from several disadvantages. The disk space on each server must be managed as an isolated island that shares resources poorly. Moreover, this solution’s expansion capability is limited by the server’s architecture. Adding more disk space can require installing an external storage unit or replacing the media with higher-capacity disks. Additionally, free space on one server cannot easily be allocated to a different server that is at or near capacity.

- **Network attached storage (NAS)**—This storage method is the preferred solution in many data storage environments where increased scalability must be accommodated in a variety of client / server platforms. It is, without doubt, the easiest and most economical way to add additional capacity, and it also provides easy connectivity to local area networks. Most preconfigured NAS storage devices have capacities ranging from a few gigabytes to several terabytes.

- **Storage area network (SAN)**—These solutions are at the highest end of enterprise storage solutions. They are easy to manage, and they provide unlimited expansion capabilities. This approach also has the advantage of concentrating all storage administration under a common management infrastructure. SANs are dedicated storage networks in which servers and storage devices are connected by hubs and switches. The network’s software suite permits the centralized administration of data regardless of platforms or media. Thus, in this open systems storage environment, separate storage devices are no longer required for each operating software environment.2

With respect to electronic records retention, the key issue is managing the life cycle of the data residing in these and other storage environments such that the right data is maintained on the right storage devices, and only for as long as required to meet business needs. An aggressive data migration strategy driven by proper data retention practices is needed. These matters are detailed later in this chapter.

**Data Archiving and Backup**

The terms data backup and archiving are often used interchangeably but are frequently misunderstood, particularly in the context of electronic records retention projects. They refer to two completely different data storage management tasks:

- **Data backup** refers to making a copy of data residing on primary, on-line storage devices onto removable media for purposes of off-line, off-site security storage for disaster recovery purposes. The intent of data backup routines is to provide the capability of recovering data when on-line processing is interrupted or when a data loss occurs.

- **Data archiving**, on the other hand, refers to the migration of data from on-line processing environments to near-line or off-line storage systems for purposes of providing for its long-term retention on storage media suitable for that purpose.3

**On-line and Near-Line Archiving**

Data archiving routines may be further defined in terms of on-line and near-line archiving. On-line archiving refers to taking data that is not being used on a regular basis and storing it efficiently on direct-access systems such as disk drives or enterprise storage systems connected via fiber or other cabling. The major benefit is achieving greater efficiencies in overall storage management through high-speed access when the data is needed. Other benefits
include reduced back-up time and reduced hard-drive requirements, which in turn, translate into reduced management, maintenance, and support costs.\textsuperscript{4}

Near-line archiving is a storage management process in which semiaactive data is migrated from the high-performance, on-line disks to slower media such as robotic tape and optical or magnetic jukeboxes. Retrieving data from near-line storage devices is slower than from on-line media but much faster than from off-line media.

These storage management solutions and functions are not, in and of themselves, electronic records retention. Again, the key issue is managing the life cycle of the data such that the right data is maintained on the right storage environment to ensure that this type of management happens.

**Hierarchical Storage Management (HSM)**

Hierarchical storage management (HSM) is a data storage strategy that has as its primary purpose the automated migration or movement of data from primary storage to secondary and sometimes tertiary devices.\textsuperscript{5} HSM is a data management strategy designed to separate active and inactive computer data by migrating files between different storage media based on predefined criteria such as access needs, available storage capacity, media cost, and other factors. This type of storage management solution has been utilized in mainframe environments for many years. During the early 1990s, the methodology was applied to distributed, client / server environments, when a number of software companies began to develop HSM software designed to operate in these environments. We mention it because it is directly relevant to the manner of deployment of electronic records retention initiatives in any computing environment that has an installed HSM solution.

Most IT departments operate on a two-tier storage scheme. Tier one, on-line storage, includes files that reside on hard disks and are immediately accessible. When those files are backed up to magnetic tape, they reside in tier two, off-line storage. An HSM strategy retains the on-line and off-line levels but inserts a third tier between them. This tier migrates semiaactive files from hard drives to more cost-effective archival media. It does not directly expand capacity, but it does provide more efficient use of storage resources, particularly expensive on-line disks.

HSM is simply a method of automatically managing the migration of data files up and down the storage hierarchy according to frequency of access by users. The administrator sets rules implemented by the software that dictate which data should be migrated from hard disk to secondary storage and when. The philosophy is to ensure that the hard disk drives never fill up. The rules select old or less frequently used files for downward migration, which occurs when the disk drives reach a preset capacity limit.

In cases where an HSM solution is installed to manage the migration and storage of data, the challenge is to ensure that retention schedules are properly integrated with the HSM migration routines. The data retention periods specified in the schedules should be constructed in on-line, near-line / off-line, and total segments, in a manner consistent with the lengths of time that data should reside during each of these phases of its life cycle. Of course, each phase, as well as the total retention, should be based on an assessment of operational requirements. This type of assessment is discussed next.

**Scheduling Production Application Data for Retention**

The following methodology is prescribed for scheduling the data in IT-managed system applications for retention, and for incorporating the retention periods into an organization’s larger enterprise records retention schedules.

Implementation of this program is discussed in Chapter 12.

To schedule the data in production applications for retention, we recommend the following seven-step methodology:

**Step 1: Obtain Cooperation / Participation of IT Department**

Electronic records retention projects cannot be accomplished without the cooperation of the IT Department. Ideally, this cooperation should take the form of a partnership in which IT staff members work together with records specialists on a multiyear initiative to make enterprise-wide electronic records retention a reality. The methodology proposed here is written, however, based on the premise that senior records and information specialists will assume a leadership role in these initiatives.

A high level of cooperation between records and IT specialists is essential at every step in the process—from identifying the electronic records that must be scheduled, developing the retention policies, and finally implementing the policies by purging the data or preserving them, as provided by the retention schedules. The first step is to enlist the support of the chief information officer and/or other senior IT managers. Depending on the size of the computing environment and the number and complexity of system applications managed by IT, these schedule development projects can take from two to six months; sometimes longer for larger organizations. Implementation of electronic records retention programs, however, typically requires a multiyear commitment on the part of IT. Implementation is discussed further in Chapter 12.

**Step 2: Collect Summary Data from IT Describing System Applications**

The most important preliminary step in planning electronic records retention projects in IT-managed computing environments is to understand the size and scope of the...
problem. First and foremost, this process involves obtaining information about the number and type of production applications the IT department manages. The following summary data about each application is needed:

- **General descriptions of all applications.** Descriptive data should include the business purpose(s) served by the applications and the data that comprise them. These descriptions should show, in some detail, the content and structure of the data contained in each production application. IT departments nearly always have this type of data readily at hand in some form or format. Frequently, this type of information is contained in an application portfolio, a systems directory, or some similar report or document describing the applications that IT manages. With this data, the records specialist will be able to plan and execute the subsequent steps.

- **Lists of data owners and applications developers.** For each application, the records specialist should obtain the name(s) of the owner of the data; that is, the manager or other professional specialist who has primary responsibility for the data for business purposes. This person(s) will usually be a manager of an operating department. Also, if the data owner does not have direct, hands-on experience in using the data, request the names of one or more end-users of applications data. Further, the name of the applications development specialist (usually assigned to the IT department) who has responsibility for each application should also be collected. A list of these persons is needed in order to send them survey questionnaires and to arrange subsequent interviews.

Also, although not as important as the previous two items, if the following information is readily available, obtain it as well:

- **Lists and descriptions of system outputs.** IT departments nearly always maintain listings of reports (hard copy and/or microfiche) generated by the applications they manage. These reports can be very helpful in identifying and analyzing all applications that need to be scheduled. Moreover, such listings are essential in ensuring that the organization’s retention schedules are complete with respect to their coverage of visible records media.

- **Lists and descriptions of tape rotation and data back-up routines.** IT departments also have this information on hand. This information is essential in developing the electronic retention schedule, because tape media contains most of the organization’s archival data at the end of its life cycle—data that will be subject to purge routines or preservation actions as reflected by the retention periods.

An example of the summary data can be illustrated as follows:

**System / application name:** Personnel Information Management System

- **Business function:** This system consists of applications containing modules of data used to manage the company’s human resources functions. Separate applications for personnel records on individual employees (active / separated); recruitment / selection and other pre-employment records; compensation and salary administration records; and employee benefits administration records.

- **Data owner:** Marilyn Smith, VP, Human Resources (HR) Dept.

- **Application developer:** Jane Doe, HR Information Systems Specialist

- **Platform:** UNIX

- **Hardware vendor:** Hewlett Packard

- **Application software vendor:** PeopleSoft

- **Database:** Oracle

- **Size / disk space:** 32 Gigabytes

- **Back-up schedule:** Nightly (Tuesday thru Sunday), and first of month

- **Type of backup:** Full system

**Step 3: Solicit Data from Applications Developers via Questionnaire**

Having obtained a general description of the system applications managed by the IT department, the next step is to conduct a survey to gather specific information about the retention status and life cycle management aspects of those applications. We generally recommend a brief survey questionnaire, to be completed by applications developers, followed by personal interviews with data owners and the developers who have completed the forms.

**THE DATA COLLECTION SURVEY INSTRUMENT**

In soliciting life cycle management data from applications developers, any survey instrument must be as brief and succinct as possible. If a respondent glances through 20 or 30 questions and realizes that more than 10 to 15 minutes for each system application will be required, response rates will be low. In most IT departments, burdensome time commitments for responding to surveys will not be acceptable. Thus, survey questionnaire forms for electronic records retention projects should be held to a few key questions on a single page if possible.

A sample one-page electronic records survey form is shown in Figure 5–1. The completion time averages 10 or so minutes per form, which is a realistic time commitment for even the busiest IT staff. The authors have used this form successfully to gather information about electronic records from applications development specialists and data owners / users in many organizations.
ELECTRONIC RECORDS SURVEY FORM

As part of the Enterprise Records Retention Project, electronic records need to be inventoried and scheduled for retention. Your assistance is requested by responding to the following questions. Please complete and submit one form for each production application.

Application: ___________________________________________________________________________________________
[If an application contains no data, write No Data and answer Question 1 only.]

Platform: ______________________________________________________________________________________________

Principal Business Owner: Name ______________________________ Department ____________________________

Form Completed by (name and title): _______________________________________ Telephone Ext: ____________

E-mail Address: ____________________________________________________________________________________

1. Briefly describe the business process or function performed by this application.
   ________________________________________________________________________________________________
   ________________________________________________________________________________________________

2. Is any provision made to identify or flag inactive records* in this application? No ☐ Yes ☐ If yes, describe the basis or criteria for inactive status.
   ________________________________________________________________________________________________
   ________________________________________________________________________________________________

3. Are any inactive records routinely archived or otherwise purged / deleted from this application?
   No ☐ Yes ☐ If yes, describe the functionality for purging inactive data and indicate when this activity occurs.
   ________________________________________________________________________________________________
   ________________________________________________________________________________________________

4. What data retention practices are currently in place for this application, if any? Please share any opinions concerning how long you believe inactive data from this application should be retained for operational or business purposes, and elaborate on the reason(s) justifying these opinions.
   ________________________________________________________________________________________________
   ________________________________________________________________________________________________

5. Are you aware of any legal issues or requirements that justify the extended retention of data in this application? Are records in this application needed to substantiate a legal reporting, taxation, or examination position?
   No ☐ Yes ☐ If yes, describe and indicate the duration of the retention to satisfy these needs.
   ________________________________________________________________________________________________
   ________________________________________________________________________________________________

6. Is this application scheduled for conversion to another platform / system? No ☐ Yes ☐ If yes, describe.
   ________________________________________________________________________________________________
   ________________________________________________________________________________________________

7. What percentage of inactive records do you estimate for this application?
   ________________________________________________________________________________________________
   ________________________________________________________________________________________________

* An inactive record is defined as any record not necessary for daily operations. It does not have to be readily available but must be kept for legal, fiscal, or historical purposes. Inactive status does not equate to automatic destruction, but it can imply movement off-line.

Instructions: Please complete by (10 days from distribution date) and return to: (name and mail station or e-mail address). If you have questions or further comments please call (name, telephone, and e-mail address). Thank You.

[Sample Form – To be completed by IT or end-user personnel]
A commentary / critique of the form, with suggestions on how it could be modified for use in any data collection effort, follows.

The Survey Form’s Data Elements

Each data element of the electronic records survey form serves a specific purpose. In this section, we describe these purposes, discuss each question, and provide other information that will help records specialists prepare a customized form that will elicit the specific information they need to define the records retention requirements for each application managed by the IT department.

Title

In good forms management / design practice, the title of the survey should be stated clearly at the top of the questionnaire, in large bold print. For our sample form, we have chosen the title Electronic Records Survey. Alternative titles might be Data Retention Requirements — by Application; Data Life Cycle Management Survey, etc.

Instructions

The first paragraph on the form should state clearly and succinctly the purpose of the form, who is required to complete it, and how to complete it. Also, indicate the senior executive who has authorized the survey to be conducted. For instance, if the questionnaire is to be completed by IT applications developers, the name of the chief information officer or the overall head of IT should be included. This name will communicate the unmistakable message that this effort is supported and sponsored by senior management and that completion of the forms is required. Forms may be sent to respondents in old-fashioned paper format; in most environments, e-mail will be the preferred method.

In cases where IT departments have project charge-back routines in place to account for this work on projects, establish a general charge-back number for the project and instruct respondents to charge any time spent completing surveys to that account number.

Name of Application / Platform

Insert the commonly used application name and any code or system numbers, if available. Platform refers to the hardware and operating system technology upon which this application system operates (for example, VAX VMS or Mainframe MVS). If good information was obtained from the general application descriptions in Step 2, this information should be inserted prior to sending the forms to respondents. Alternatively, the application or platform information may be left to the respondents to complete.

Principal Business Owner(s)

In cases where application data has a single business owner, this information is straightforward. However, in cases where application data is shared by multiple business functions, the response can be more complicated. This information is important, however, to further identify applications and for follow-up interviews / surveys with those business users.

Respondent’s Identifying Information

This information about the person completing the form (name, title, telephone number, and e-mail address) is needed for follow-up questions and for scheduling interviews.

Comments about Specific Questions

Question 1 – Business process / function of application. Briefly describe the business process or function performed by this application.

For relatively simple applications, one to three or so sentences that clearly and concisely explain the function and purpose of the application and the data residing in it should be sufficient. In cases where applications are structurally complex and consist of multiple modules of data, each serving a distinct function, detailed descriptions will be needed.

Question 2 – Data flagging. Is any provision made to identify or flag inactive records in this application? If yes, describe the basis or criteria for inactive status.

This question is necessary to understand how and when the data makes its life cycle transition from active to semiactive or inactive status, and whether the system has any flags that manage these status changes.

A data flag, then, is a software utility for identifying the point in time when electronic records make their life cycle transition from an active to a semiactive or inactive state. This status change may indicate that the records are eligible for migration from primary to secondary storage media.

An inactive record is defined as any record not used in daily operations. It does not have to be readily available but must be kept for legal, fiscal, or historical purposes. Inactive status does not necessarily indicate immediate destruction of the data, but it can imply movement off-line.

Question 3 – Purge routines. Are any inactive records routinely archived or otherwise purged / deleted from this application? If yes, describe the functionality for purging inactive data and indicate when purging occurs.

In cases where application data is of temporary value, this question is needed to ascertain whether any software functionality exists to recognize expired data and remove it from the environment according to the approved retention periods. This information is probably best known to IT application developers, although data users may have some insight into the life of their data, and when, if ever, it is purged from the system.

Data purging is the automatic erasure of useless electronic records, effectuated by means of purge functionality, based on predefined electronic retention periods that have been incorporated into the design criteria of a computer
application. Purge functionality is any set of programmed instructions, either built into applications programs or as a system-wide utility, to identify expired data and effectuate its disposal. These actions should occur under the authority of an electronic records retention schedule. A detailed discussion of data purging is in Chapter 12.

**Question 4 – Current and recommended retention practices / needs.** What data retention practices are currently in place for this application, if any? Please share any opinions concerning how long you believe inactive data from this application should be retained for operational or business purposes, and elaborate on the reason(s) justifying these opinions.

This question is needed to determine whether any current data retention practices exist for each application and if so, whether they are adequate to meet the operational / business needs of the organization. In cases where no such practices exist, this question solicits the opinions of whoever completes the form as to what retention period is believed to be in the best interest of the organization. The application development specialist will usually have some general or specific knowledge about current retention practices.

Of course, the quality of the information and judgments concerning this matter are likely to vary widely. In some cases, excellent data and valid opinions will result; in other instances, less so. The intention is not to ask for their definitive decision or final word on records retention, but rather to gain information about current operational needs and requirements as a basis for discussions of this most important matter during a subsequent interview.

**Question 5 – Retention value for legal / audit purposes.** Are you aware of any legal issues or requirements that justify the extended retention of data in this application? Are records in this application needed to substantiate a legal reporting, taxation, or examination position? If yes, describe and indicate the duration of the retention to satisfy these needs.

Frequently, the applications developers who often complete these survey forms will not possess anything other than superficial knowledge concerning how long applications data must be retained to satisfy statutory or regulatory requirements. Or how long such data should be retained to meet other legal needs. Data owners generally have somewhat better knowledge on this subject. We think this question should be asked on this survey form, however, as it gets the issue of legal requirements / value on the table and serves as a point of departure for in-depth analysis in the ensuing steps. See Step 5 in this chapter as well as Chapter 3 for more on the legal aspects.

**Question 6 – Future system conversion.** Is this application scheduled for conversion to another platform / system? If yes, describe.

The purpose of this question is to begin collecting the data needed to plan for implementation of the electronic records retention program, which requires the integration of data purge routines into all applications that need it. Conversion to new platforms or systems is usually the best time to introduce purge routines. For instance, if a number of legacy applications are scheduled to be migrated from a mainframe base to a client / server environment, building in purge routines sufficient to execute the retention policy at the time of conversion if they do not exist is advisable. Inactive data can be purged at this time also. See Chapter 12 for further discussion on implementation.

**Question 7 – Percentage of active / inactive files.** What percentage of inactive records do you estimate for this application?

This question is necessary to gather data for purposes of building the business case for electronic records retention. Recall that in Chapter 2 we indicated that a major element in this case is the percentage of the organization’s total quantity of stored data that is useless and that could be destroyed during year one and in subsequent years of implementation of the retention initiative. Good responses to this question constitute the first step towards determining the quantity and cost of this disposal as a basis for calculating the benefits of enterprise electronic records retention. Usually applications developers can estimate the percentage of inactive records in the applications they manage.

**Survey Return Information**

The concluding portion of the electronic records survey form contains instructions for respondents as to when the questionnaires must be completed and where to return them. Short response times are generally better than longer ones. Seven to ten days from the mailing date should allow sufficient time for respondents to complete and return the forms. Always give a name and telephone number to contact if respondents have questions. Include the name and mail code / address for returning the form after completing it.

**Test the Survey Form**

In many instances, testing the survey form prior to its actual use is advisable. To test the form, the records specialist should complete it and record the amount of time required to complete it. Departmental associates also should complete forms, noting how long to complete and any questions they have. Further, recruits from the IT community (as well as some data owners / users) can make up a small sample group. Their timing, comments, and suggestions may be used in refining the form. The estimated time to complete a questionnaire may be printed on the form. If the review process reveals that twenty minutes are needed to complete one form, perhaps questions need to be streamlined or limited so that less time is needed to complete the form. One respondent may be responsible for completing a dozen or more forms; therefore, it should not become an unduly time-consuming exercise.
Survey Response and Follow-up

Response rates to this type of survey questionnaire will vary. Although a 100 percent return of all questionnaires sent out is obviously the goal, such a high return is not always possible. The records specialist or other members of the project team should follow up with those individuals who have not returned forms after the return date. Telephone calls, notes, or e-mail can remind them that forms are past-due. Determine whether contacts are having any particular problems completing the form, whether they are on vacation or otherwise unavailable, or whether the forms should be directed to someone else. Gentle prodding, without badgering respondents, may be required to get compliance. Keep a running log of who has returned forms. As the return date approaches, start calling or issuing reminder notes that survey forms are due.

Summarize Results

When all, or as many as possible, forms have been returned, the survey data should be compiled for further analysis. Analysis of the survey data can be maximized by following two important steps:

1. Build a database or spreadsheet of verbatim responses that can be manipulated, printed, and statistically analyzed.
2. Plan for each form element to be individually fielded to maximize sorting and manipulation.

Once the results have been compiled, the current status of enterprise electronic records retention will be known, possibly for the first time in the history of the organization. A summary report sent to the organization’s senior management will inform them of this important event. The focus of the report should be on what the survey results imply about the business case for enterprise electronic records retention. Use the survey results to build this case based on the concepts presented in Chapter 2.

Step 4: Conduct Interviews with Applications Developers and Data Owners / Users

Having collected the survey data, the records specialist now possesses summary information concerning the content, use and purpose, and current retention / life cycle management status of the data residing in every production managed by the IT department. The next step is to validate and supplement this information by conducting personal interviews with persons who are in the best positions to provide valid input as to how long the data should be retained and whether and how expired data can be disposed of; i.e., the owners and users of the data and the IT developers who manage the applications.

If retention specialists can get these parties into the same room at the same time, and if the discussion is intelligently handled, good decisions can be made concerning how long the data should be retained in all applications.

These interviews have four primary purposes:

1. To validate the data contained on the survey forms for each application;
2. To define the electronic records series—the schedu-
able bodies of data contained in each application;
3. To define the retention values of each electronic records series and to make preliminary retention decisions for each;
4. To discuss strategies and functionality for implementing the retention periods.

These four purposes or substeps are discussed next.

Substep A: Validate / Supplement Survey Data

For each application, review the survey forms to determine whether valid data has been collected for each of the following:

1. Name of the application
2. Business purpose / function of the application
3. Nature of the usage of the data
4. System manager and information owner(s)
5. Hardware platform
6. Software environment
7. Content, organization, and structure of the data
8. Time span of the data
9. Size and growth of the data
10. Location(s) of data storage (on-line, near-line, off-line) on various media types
11. Use and format of data or reports generated
12. Description and purpose of output
13. Nature and frequency of data archiving and back-up routines

Substep B: Define the Schedulable Records Series

Discuss the structure of the data contained in each application, and define the electronic records series—the separate, discrete bodies of data that require a separate retention period in order to provide for the proper retention and life cycle management of the data. To put it another way: Is disposing of all the data in this application after x period of years feasible, or do various modules of the application data have different retention requirements and will therefore need separate retention periods? As discussed in Chapter 4 (Principle No. 2), establishing only one retention period to provide for the disposition of all data in a single application will often be feasible. In other cases, owing to the content, structure, and usage of the data, multiple retention periods may be required.

Eliminate Applications Containing Pass-thru Data

During the data collection exercises described previously, developers will frequently provide descriptions of applications that have been established for the sole purpose of feeding data into or out of other applications. These types of pass-thru applications are typically developed by IT
departments to build an interface with other applications. However, because they are not themselves repositories for retained data, the pass-thru data in them would not be considered to be schedulable. Thus, they can be eliminated from further consideration for purposes of retention analysis and schedule development.

These types of applications are generally identified by software developers as they describe the nature of their applications and the data contained in them during the interview process. Alternatively, they can be spotted earlier and eliminated from analysis. If desired, the instructions on the data collection form can advise those completing it that forms are not necessary for any applications of this type. Note that, in some computing environments, these applications constitute a fairly significant percentage of the total—perhaps as many as 25 percent in some environments.

Consider a General Retention Schedule for IT Administrative Records. Organizations should consider developing a general retention schedule to provide for the disposition of certain administrative and management records typically retained by IT organizations in executing their responsibilities to develop and operate an enterprise technology infrastructure. With its issuance of General Records Schedule (GRS) 24 (currently proposed and under review by federal agencies), the U.S. National Archives and Records Administration has taken this approach. This schedule provides retention and disposition authority for the following categories of electronic records:

- IT facility, site management, and equipment support services records
- IT asset and configuration management records
- System backups and tape library records
- Records related to maintaining the security of systems and data
- User identification, profiles, authorizations, and password files
- Computer security incident handling, reporting, and follow-up records
- IT operations records
- Financing of IT resources and services records
- IT customer service records
- IT infrastructure design and implementation records
- Electronic mail and word processing system copies

To the extent that these records exist in most if not all IT departments, they can be scheduled for retention under an approach similar to that utilized in the proposed GRS 24.

Substep C: Make Preliminary Retention Decisions
Discuss the business value of the data contained in each electronic records series, and solicit an opinion as to how long it should be retained to meet the operational needs of the business. The overriding goal is to develop retention periods that are managerially reasonable; that is, not too long, not too short.

The various methodologies for making these decisions discussed in Chapter 4 (Principle No. 3) should be employed to guide this discussion. The following questions need to be answered for the schedulable records series in each application:

- How long is the data kept / needed on-line, off-line? How long is it kept / needed in manipulatable form? A valid answer to the latter question will generally equate to the total retention period for each records series.
- What is the value of the data to the organization? Define and quantify both the short and long-term value—operational and reference value, fiscal or audit value, legal / regulatory values, and historical / archival values. How does each value decline over time and when does each expire, if ever?
- What is the shortest retention period possible for the data in this application? What is the longest? With which time period between these two extremes are we most comfortable?

Substep D: Determine the Functionality for Retention Implementation
For each application in which the data is deemed to be of temporary value (that is, it will be disposed of), determine whether the software used to process it has purge functionality sufficient to effect its proper disposal. If not, discuss whether, when, and how such functionality can be incorporated into the technology environment. See Chapter 12 for a detailed discussion of this matter.

In those few cases where the data is judged to be of enduring value and needs to be retained in computer-processible form permanently or for lengthy periods of time, determine whether sufficient practices are in place to satisfy this requirement. See Chapter 11 for a detailed discussion of technical guidelines and best practices for long-term data retention.

At the conclusion of these interviews, the schedule development team will have defined the records series for all applications, made preliminary retention decisions as to how long the data for each series should be retained, and determined whether sufficient data purge functionality exists in the software environment to implement the retention periods. The next step is to determine whether any laws or regulations exist that may have an impact on the retention of the application data.

Step 5: Determine Legal Retention Requirements
As with all other records, retention periods for electronic records must be in compliance with the law. Thus, the purpose of this step is to determine whether any arm of the government imposes any laws or regulations that mandate that the data for each application be retained and if so, for how long. The only way to answer these questions is to
conduct legal retention research to locate any and all relevant requirements. Because approximately 10,000 to 20,000 separate records retention requirements are in U.S. law alone, this research can be a burdensome task. For U.S. laws and regulations, purchasing special legal research software that contains records retention laws and regulations in a searchable database is best. Such products are available from several vendors. If the applications data is subject to international law, customized research will usually be required as these laws and regulations are very difficult to obtain. The following are some examples of these rules and regulations:

- U.S. Internal Revenue Service – As provided by 26 CFR 31.6001-5, employers are required to keep records of all remuneration paid to employees, which include records of employees (name / address, dates of service), remuneration, noncash remuneration, remuneration in the form of tips, tax collected, W-4 and W-4E forms. The records must be retained for the current year plus four additional years.
- U.S. Department of Labor – As provided by 29 CFR 516.6, employers are required to retain basic employment and earnings records including timekeeping records, wage rate tables, records of additions to or deductions from wages paid. The records must be retained three years from the date of last entry.

As you review these and other laws and regulations, keep in mind that they may apply to, but they do not usually specify electronic records as an authorized or required retention medium. As with these two previous examples, almost all laws and regulations that require records to be retained are silent on the issue of which recordkeeping medium may or must be used to satisfy the government’s requirements. In the case of these examples, organizations typically retain payroll records in multimedia formats. Thus, requirements that appear to be relevant based on their subject matter cannot be ignored just because they do not specifically state that they apply to electronic records.

Once all relevant requirements have been obtained, the next step is to match or link them to the appropriate electronic records series and ensure that the preliminary retention periods formulated during Step 4 are long enough to comply with them. In most cases, the retention periods established to meet operational or business needs will exceed any government-imposed retention requirements.

In all cases where applications data is governed by a legal retention requirement, the citation for that law or regulation should appear alongside the records series in the retention schedules, as discussed in Step 6.

**Step 6: Integrate Electronic Retention Periods into Enterprise Retention Schedules**

At this stage of the project, you now have a listing of all electronic records series comprising the schedulable data in all system applications, you have assigned preliminary retention periods to each of them, and you have conducted research to confirm that these retention periods comply with the law. The next step is to integrate these electronic records series and their retention periods into the organization’s enterprise retention schedules. Retention periods for electronic records should be added to the existing records retention schedule in the same form and format as any other organizational record. With respect to form and format, three main options are available:

1. **Develop media-specific retention schedules.** This format option consists of separate schedules for electronic records as well as for those on visible media. Under this option, readers know whether they are reading the schedule for electronic records as opposed to the one for physical records. This option is acceptable, but it is not generally preferred. See option 3.

2. **Develop media-independent retention schedules.** This format option consists of schedules that list various records series, without reference to storage media. This approach is justified as the records for a given series may, in fact, reside on several media simultaneously or during various stages of their life cycle. The theory here is that applying consistent retention policies for duplicate data on multiple media is better and that storage media has no relation to retention period. This option is not recommended, for reasons discussed in Chapter 4 (Principle No. 6).

3. **Develop multimedia retention schedules.** Schedules that list all media, with separate retention periods for the information resident on each media. This option is generally recommended as it provides the clearest advice for those who must implement the schedules in a multimedia recordkeeping environment.

The retention schedule for visible media records typically has fields for the record name, user department, record description, and perhaps a control number; these same fields are appropriate for electronic records. Also particularly appropriate are fields describing the location of records as they age; that is:

- **The active / in-department field.** This field indicates the time during the stage of the records’ life when they should remain in the active office area, which equates to on-line for electronic records.

- **The in-storage field.** This field indicates the time the records spend in inactive records storage, which is analogous for inactive electronic records when they are migrated off-line, or on-tape.

**Step 7: Finalize Retention Periods and Publish Schedules as Organizational Policy**

Once the preceding tasks have been completed, the final step is to obtain management approval of the revised retention schedules, finalize the retention periods based on any requested revisions, and issue them as organizational policy.
In most organizations, this step is handled by submitting the retention schedules to the several senior management officials who have a direct and legitimate interest in enterprise records retention matters. These officials include:

- **Managers of departments or business processes.** By approving of the retention periods for electronic and other records for which they have management responsibility, these managers are giving their consent that the retention periods meet the operational requirements of the business.

- **Legal counsel.** By approving of the retention periods for electronic and other records in the schedules, these attorneys are giving their consent that the retention periods are sufficient to meet the legal retention considerations of the organization; that is, they comply with the law, provide the organization with the information it needs to defend itself against lawsuits or prosecute suits brought against other parties, and meet the organization’s other legal needs. To facilitate this review, we recommend submitting the results of the legal research and the list of citations linked to relevant records series for review by legal counsel.

- **Chief fiscal officers and/or tax managers.** By approving the retention periods for financial records and tax documentation, these managers are giving their consent that the retention periods for electronic and other records are sufficient to meet the organization’s audit requirements and other tax and fiscal accountability needs.

**NOTES**


5. Ibid., “Migrating Data with HSM.”

Some twenty years have passed since the personal computer (PC) revolution began its conquest of the desktops of office workers. Prior to that time, very few such workers had ever had any direct experience with computers. They had certainly not created business records on such devices. Now, two decades later, PCs occupy the desktops of virtually every office worker throughout North America, and untold millions of electronic records are created on these machines by their users every business day.

What happens to these records during the course of their life cycle? Are they permitted to languish indefinitely on the hard drives of their host machines or on a network server until they are forgotten about? Or are they systematically destroyed under an established records retention program based on retention times commensurate with their value? Our premise is that the latter method of records disposition would definitely be in the best interest of the business that employs these office workers and owns these desktop computers. However, if the records are casually kept and are disposed of at the discretion of their creators, how can policies and practices be put into place to bring some professionalism to electronic records created at the desktop level and under the control of the end-users? This chapter addresses these matters.

DESKTOP RETENTION: MORE CHALLENGING THAN PAPER!

To obtain a grasp of the difficulties associated with applying records retention practices at the desktop level, let’s first draw some comparisons with paper records stored in file cabinets. If these records are well managed, they are organized in file folders and housed in file drawers in a logical sequence that corresponds to records series appearing in the records retention schedules. Further, the records series are frequently segmented by date; that is, by year of creation. Thus, to correctly apply the retention policies to these records is a relatively easy and efficient matter: The custodian simply removes the entire series—all the file folders in all cabinets for a given year—and either effects their immediate disposal or boxes them and transfers them to storage, as required. To thus apply retention to the contents of several cabinets would typically require no more than an hour or two, during which time the custodian would have properly disposed of literally thousands of paper documents.

With PC-based electronic records, the situation is frequently much more problematic and difficult. In the absence of guidance concerning how to organize and label electronic documents in desktop computing environments, PC users are left to their own devices to organize the records they create into schemes of their own invention. Frequently, they will store documents using filenames that are arbitrarily chosen, cryptically expressed, and known only to themselves. Further, these documents are often organized in directory listings in a straight alphabetic sequence, without regard to categories that correspond to the records series appearing in the organization’s records retention schedules.

In short, in the absence of formal records management and retention practices, individual office employees are free to manipulate files—to create, store, modify, delete, and destroy records—at any time, entirely at their discretion, without rules or discipline, and without complying with any established records retention requirements.1 Unless PC-based records have been logically organized by directory / subdirectory into categories corresponding to their retention status, unless automated tools and utilities are in place to accomplish data purging based on the retention schedule, the process of applying any retention policy to these records is even more cumbersome and time-consuming than in paper-based recordkeeping environments.

PC-based records present special records retention challenges because PC users often consider these records to be personal working files, to be used and disposed of at their discretion. In fact, this perception does have some truth to it; the records management goal is to embody it into the organization’s records management policy and endeavor to implement this policy as aggressively as possible. Conducting a detailed inventory of all PC-based records retained by most organizations is simply not practical. Thus, records managers must pursue a simpler approach to retention planning and implementation for these records. The following general principles governing the retention of desktop records are designed to facilitate this process.

General Principles for Desktop Records Retention

The following principles are recommended as the basis for records retention policies related to retaining and disposing
of PC-based records residing on desktop and portable computers. These principles have been embodied in the sample policy appearing in Figure 6-1.

- The responsibility for retaining and disposing of PC-based electronic records should generally reside with individual employees. As discussed in Chapter 8, in some recordkeeping environments utilizing records management or electronic document management software solutions, some of this burden can be shifted. Generally, however, individual employees should be responsible for reviewing their PC-based records periodically in order to make judgments concerning their retention and disposal, under established policies and procedures, such as those enumerated in this section.

- The retention of PC-based electronic records should be content-driven. A single retention period will not realistically apply to all PC-based records. Further, if the content of any given PC-based document or record relates to an established records series appearing in the organization’s records retention schedules, the retention period for that records series would govern the retention of that record.

- The organization’s records retention schedules should include all records of official character and/or operational importance. If discrete groups of records of this nature happen to reside in PC-based computing environments, they constitute separate records series, and they should be scheduled for retention and listed on the retention schedules.

- Although many exceptions can be found, as a general rule, PC-based electronic records possess relatively short-term retention value. Nearly all such records have retention value for less than five years, and most have value for only a year or two. Nearly all records used by desktop users in their daily work are less than three years old.

- Desktop records purge days are strongly recommended as the single most effective strategy for implementing records retention policies for PC-based records. These purge days should be conducted one or more times each year, as prescribed in the sample policy appearing in Figure 6-1.

### Official vs. Nonofficial Records

Increasingly, the question “What is a record?” is one of the most troubling conundrums in records management.\(^2\) This issue is particularly relevant to the matter of desktop records retention. The form or format of a record object is irrelevant for records management purposes; as noted previously, the content determines whether a message of any type is considered a record. An official record is one that captures and maintains a record’s content, structure, and context through its full retention period, in a manner that is fully sufficient to provide evidence of a business activity. To be considered official, an electronic record must be produced by an electronic system in which records are collected, organized, and categorized to facilitate their preservation, retrieval, and disposition. Nonofficial records, on the other hand, are those that are typically used to create official paper or microfilm records.\(^3\)

Finally, distinctions between official and nonofficial records have no legal / judicial significance. In an evidentiary context, the courts normally do not differentiate between official records and nonrecords. If the content of any extant information object is deemed relevant to legal proceedings and is, in fact, requested under subpoena or other judicial order, it must be produced. If it is not or cannot be produced, the court will demand an explanation. If the explanation is not sufficient, the owner of the record could be liable to fines and/or other judicially imposed penalties, up to and including imprisonment. See Chapter 3 regarding legal issues.

### Executing a Desktop Retention Methodology

Chapter 2 presented what we believe to be a fallacious argument as to why desktop retention is not practical. We indicated that we reject the notion that organizations should ignore desktop retention as impractical. With respect to a hypothetical cost scenario, consider the following metrics:

- The typical desktop user creates from zero to three documents per day on PCs or portable computers. This figure includes word processing documents, spreadsheets, and presentation graphics documents but excludes e-mail, which should be considered a separate issue for purposes of managing desktop records.

- For purposes of this exercise, we will use an average of two documents per user per day, which is conservative, based on our experience. Thus, based on 260 workdays per year, the annual accumulation would be a total of 520 documents.

- To apply retention policies to these records, the desktop user is required to open all documents, briefly review their contents, make a judgment as to their retention status based on published policies and procedures, and then execute the disposal of all those eligible for this action. We estimate these tasks at three minutes per document. On this basis, the annual burden of applying retention policies to desktop documents, exclusive of e-mail, would be 26 hours.

- If desktop users are required to review their documents four times each year during quarterly desktop purge days, the retention burden would be 6.5 hours per quarter.

We acknowledge the reality that no records retention policy, in any recordkeeping environment, can ever be implemented to perfection. Some desktop users will cling to the every-conceivable-contingency syndrome and fail to apply retention to their PC-based documents as aggressively as may be desirable. We contend, however, that the fact that a
desktop retention methodology will not be executed to perfection is not a reason for not doing it! A good desktop retention policy, aggressively implemented, should be 80 percent successful. Only 20 percent of the documents eligible for disposal have not, in fact, been destroyed, while the remaining 80 percent of all documents eligible for disposal have been properly destroyed.

The organization’s senior management would, of course, need to make a judgment as to whether the benefits of implementing a desktop retention methodology—one which has as its goal achieving 80 percent full compliance with the retention policy—is worth the cost. As advocates for electronic records retention, we believe it is.

**DESKTOP USERS’ GUIDE**

Most if not all organizations of any size should develop a *Users’ Guide to the Management of Electronic Records at the Desktop Level* as one of its major strategies for improving the management of PC-based electronic records. Very few desktop users in the U.S. have this kind of guidance furnished to them, and we think it is critical if PC-based records are to be managed in accordance with professional records management principles and practices.

The table of contents of this type of procedure would typically consist of the following:

- Purpose of this Guide
- Filing Records Created by Desktop Applications
- Protecting Records Created by Desktop Applications
- General Retention Policies for Electronic Records
- Retention of Records Created by Desktop Applications
- Responsibilities for Disposing of Electronic Records
- Records Management Practices for E-mail
  - Saving E-mail
  - Deleting E-mail
  - Using AutoArchive to Delete Messages
  - Using AutoArchive to Save Messages

This best practice guideline should be posted to the organization’s Web site, and training sessions on its content should be offered to all employees.

---

**RECORDS RETENTION AT THE DESKTOP LEVEL**

During the past several years, ABC Corporation has provided desktop and/or laptop computers to virtually all its office employees and many production employees as well. In fact, the thousands of these machines now in use in the company are being used to create a substantial portion of the company’s electronic records. Thus, ABC employees need to be furnished with clearly defined policies and procedures concerning recordkeeping in this environment. This document addresses this need. This document is designed to be used in conjunction with ABC’s Records Retention Schedules and with the *Users Guide to the Management of Electronic Records Residing on Desktop and Portable Computers*, which contains more detailed user guidelines than those appearing here.

**General Principles**

- **Records as assets.** PC-based electronic records created, received, or maintained by ABC Corporation may contain information essential to the company’s mission, long-term goals, and ongoing operations. Like other assets, the company’s recorded information requires systematic management based on formalized policies and practices.

- **Ownership of records.** ABC Corporation is the owner of all PC-based electronic records created, received, and/or maintained by company employees in support of the corporate mission, business operations, and other activities worldwide. They are company property. The company’s ownership further extends to PC-based records created, received, and maintained by third-party contractors that pertain to corporate operations and activities. These records, too, are subject to these policy guidelines.

- **Policy authority.** As the owner of its records, ABC is solely empowered to establish policies and procedures for the storage, retrieval, retention, destruction, distribution, control, protection, or other management and use of such records; in this case, those records residing in PC-computing environments. This policy addresses these matters.

- **Personal / private files.** Corporate ownership and authority extend to any and all PC-based
records created, received, and/or maintained by individual employees in the course of, or pertaining in any way to, company business. So-called personal working files—those related to work-in-process—may be established on company-owned PCs for the convenience of individual employees, but it is done without any connotation of personal ownership. Such personal files are company property. Private files—those not pertaining to company business—may not be created and maintained on ABC computers.

Personal Responsibilities

All employees who create and use PC-based records and information are responsible for the following:

- Maintaining all PC-based records in a manner designed to ensure their accessibility, integrity, confidentiality, authenticity, and usability for any and all business purposes.
- Maintaining proper security over all PC-based records. All PC-based records created, received, and/or maintained on ABC computers will be accessible to the company’s employees on a need-to-know basis pertinent to specific work responsibilities. The company’s information security policies will govern access and security over these records.
- Organizing and indexing all PC-based records in a manner designed to facilitate their efficient access and use, not only by their creator but also to other company personnel who may be required to use them.
- Effecting the regular and systematic disposal of PC-based records, in accordance with the company’s Records Retention Schedules and with these and other policies and procedures.
- Halting promptly the disposal of relevant PC-based records upon notification of a litigation hold by the Legal Department. The hold means that information contained in the records is or may be subject to production under a subpoena or document discovery order issued by proper authority and that disposal under authority of the retention schedules is not authorized.

User Requirements

I. Organizing and Filing PC-Based Records

Just as with paper records, PC-based records saved for possible reuse or other purposes should be filed in an organized and logical arrangement to facilitate future retrieval when needed. The following procedural guidelines should be employed:

- PC-based records should be organized into directories, which are known as folders in the Windows operating system. Folders are designed to organize or group related records pertaining to specific business activities or subjects. Folders must be created to store groups of related records.
- Separate folders should be created for specific projects, programs, or other business activities. Folders can, in turn, be further organized into subfolders that are used to store related subgroups of PC-based records, based on document type, content, date, retention periods, or other criteria. Folders and subfolders are used to organize and group related records. Unrelated records should not be intermingled within folders and subfolders. The scheme for these folders and subfolders should be consistent with the organization’s file plan and/or its records retention schedules.
- These folders may reside on a network drive or the employee’s desktop drive. Within each folder, individual subfolders might contain specific types of project-related records such as correspondence and reports (Word documents), budgets (Excel documents), and presentations (PowerPoint documents).
- Folder and subfolder titles must clearly and accurately indicate the purpose, content,
and characteristics of the records they contain.

For additional guidance concerning organizing and filing PC-based records, see the Users’ Guide to Managing Electronic Records at the Desktop Level. This publication contains specific instructions detailing how to accomplish all requirements.

II. Retaining and Disposing of PC-Based Records

Company Retention Policy  ABC Corporation hereby declares that it will manage the life cycle of its PC-based records and information by implementing an enterprise-wide records retention process. All PC-based records and information shall be retained and destroyed only in accordance with the retention periods specified in the company’s Records Retention Schedules and with this and related polices and procedures. These schedules are the company’s official policy for information retention and disposal, and they have been developed in accordance with all applicable laws and regulations and good business practices. Compliance with them is mandatory.

Retaining PC-Based Records: General Principle  Although many exceptions may be found, as a general rule, PC-based electronic records possess relatively short-term retention value. Nearly all such records have retention value for less than five years, and most have value for only a year or two. All PC-based records must be retained and disposed of based on their content, their status as official records, and their value to the company. In making decisions concerning how long to retain PC-based records, employees should first check the Records Retention Schedules and ensure that they are in full compliance with them. Most other PC-based records may be disposed of at the discretion of employees under the policy guidance provided below.

- Records of official status. If PC-based records consist of the only copy of documents of official character, then they possess status as official records and may not be disposed of except in accordance with the Records Retention Schedules. To further clarify this principle, if the content of PC-based records relate to an established records category appearing in the Records Retention Schedules, they must be retained for the period of time specified in said schedules. In such cases, employees have the option of retaining the records in electronic form, or they may produce printed copies for retention in the company’s paper files. All other PC-based records are of nonofficial character and may be disposed of as provided below.

- Records of nonofficial status. If PC-based records consist solely of electronic documents and data used to produce documents of official character retained elsewhere, then these PC-based versions would not themselves possess status as official records and may thus be deleted at the discretion of the user. They should be destroyed as soon as they are no longer needed to produce updates or revisions to official documents, and in no event should they be retained longer than the official versions of the records. PC users are encouraged to review their electronic documents and files weekly, and delete all unneeded documents and data from both removable and nonremovable media (i.e., hard disks, network servers, and floppy disks). Such actions are required of all employees during Desktop Records Purge Days (see below).

PC-Based Records Related to Litigation or Government Investigation  If the content of a PC-based record is related to actual or pending litigation or a government investigation, it may not be destroyed without the prior written consent of the Legal Department. Employees who violate this policy are subject to disciplinary action by the company, up to and including dismissal, and/or judicial penalties imposed by courts of law.
Implementation

Desktop Records Purge Days
All departments and business units are responsible for conducting one or more Desktop Records Purge Days each year. During these days, all employees are required to review all PC-based records and files under their custody (including e-mail) and effect the disposal of all records eligible for such action as provided by the Records Retention Schedules and this and related policy and practice guidelines. Records eligible for disposal will be deleted / purged from all storage media under user control—hard disks, network servers, and removable diskettes.

All employees using desktop or portable computers are required to accomplish three main tasks on Desktop Records Purge Days:

1. All PC-based records of an official character eligible for disposal will be destroyed. The manner of disposal will be sufficient to maintain the security and confidentiality of company information.

NOTES


4 This sample policy was assembled from project work on various consulting engagements in which the authors have been engaged during the past several years. We are particularly indebted to Dr. William Saffady for developing the desktop user retention requirements and responsibilities data during the course of one such engagement.
Electronic mail (e-mail), as we know it today, is now 30 years old. In 1971, Ray Tomlinson became the first person to send a message from a computer on one network to a computer on another network.\textsuperscript{1} From its humble beginnings e-mail has become, during the last ten or so years, one of the most business-critical computing applications. E-mail has literally revolutionized the way business is conducted throughout the world. In fact, we think a good argument could be made that, as a tool for business communication, e-mail ranks with the telephone as one of the greatest inventions ever. The records management implications of e-mail have been equally significant. In fact, according to some observers, management and retention of e-mail constitutes the biggest, and certainly the most pervasive, records management problem in the U.S.

E-mail has been the fastest growing business technology of the past decade. E-mail has become so prevalent in today’s organizational environment that it has become the de facto tool for enterprise-wide communication and collaboration. E-mail has actually replaced paper correspondence during the last few years. According to an article in \textit{Computerworld}, in 1996, more e-mail was sent than postal mail in the U.S. for the first time.\textsuperscript{2} Transmitting an electronic document across geographic distances is nearly always, faster, easier, and less expensive than to use postal services or private couriers.

### A BUSINESS-CRITICAL APPLICATION

E-mail today is more than just a communications medium. Corporate e-mail systems, such as Microsoft Exchange, have become long-term stores of critical business information. Creative Networks of Palo Alto, California, reports that 60 percent of business-critical information is stored within messaging systems. Moreover, about one-third of the information used daily by employees of large organizations resides within the e-mail messaging environment.\textsuperscript{3} E-mail continues to grow in importance. The article in \textit{Computerworld} referred to previously indicated that, over the next few years, messaging systems will be woven into virtually every major application that businesses use. The authors predict that, during the next several years, we will witness the convergence of e-mail, voice mail, mobile messaging, fax, and other technologies that combine features of communications, messaging, and recordkeeping.\textsuperscript{4}

### THE MAGNITUDE OF THE E-MAIL PROBLEM

The following statistics were gleaned from various information technology publications.\textsuperscript{5} They illustrate the dimensions of the information and records management problems resulting from explosive use of e-mail by business organizations.

- **Total message quantity** – According to a report by the International Data Corporation, the number of e-mail messages sent worldwide in 1995 numbered 101 billion. By 2000 this figure had increased to 2.6 trillion, and by 2005 the number of messages is predicted to exceed 9.2 trillion. Another study indicates that e-mail usage in the U.S. will grow from the current 3.2 billion messages per day to over 9 billion per day by 2003.

- **Message quantity per user** – Studies indicate that today’s e-mail users send about 15 messages per day and receive about 20 messages each day. These quantities are expected to increase by some 60 percent and 80 percent respectively over the next year. Other studies report still higher figures. An article in \textit{Business Week} cites the results of a Gallup poll conducted in May, 1998, that indicated that a typical office worker sends and receives an average of 60 e-mails each business day.

- **User time consumption** – According to a study by Gartner, Inc., the average e-mail user in 2000 devoted about 90 minutes per day to mailbox-related tasks. The study further indicated that this figure is expected to increase to 2.5 hours per day by the end of 2002. Two and one-half hours are nearly one-third of the entire working day.

- **Average message size** – A recent study by the Midrange Performance Group indicated that the average size of an e-mail message has now exceeded 50 kilobytes. Another study indicates that the average size of an e-mail message is 18,500 bytes and growing.

- **Storage burden** – The average e-mail user will attempt to store and retain approximately 500 megabytes of e-mail per year. On this basis, an organization of 3,000 e-mail users would require over 1.5 terabytes of additional storage per year. IT managers have forecast a growth of 50 percent in their message storage requirements over the next 12 months. According to some observers, this figure could be
grossly underestimated—growth rates for message stores of 100 to 150 percent may not be unrealistic.

**E-mail Mismanagement**

Clearly, e-mail is badly in need of serious management attention in many organizations, particularly the larger ones. However, despite many efforts to upgrade the quality of management for enterprise e-mail systems, e-mail continues to be undermanaged, if not mismanaged, in many organizations. From a records management perspective, the biggest single problem is that e-mail systems, which are essentially electronic post offices, are frequently misutilized as repositories for electronic archives. The use of an e-mail system should be restricted to performing its central function of facilitating daily electronic communications. It should not become the de facto repository for long-term preservation of inactive messages, the value of many of which has long since expired. In other words, the post office should not be morphed into an archive.

E-mail is frequently perceived by its users to be much less formal than a paper letter or memorandum and thus it is frequently considered insignificant once it has accomplished its original purpose of simple communication. Thus, many users typically give little if any thought to the question of how long e-mail should be retained. Once a message has been read, the user often presumes that its treatment should be like that of voice mail.

E-mail users are typically left to manage large volumes of messages on their own, with little or no policy and procedural guidance and few management tools. How do employees know whether and under what circumstances e-mails require management as organizational records? Even if these judgments can be properly and consistently made by most or all e-mail users, the question then becomes how to apply records management principles to assure their proper management. Finally, what tools are required and/or available to do this management?

What about IT departments that are responsible for acquiring and maintaining the technology infrastructure for e-mail? Unfortunately, these departments frequently view the e-mail problem, superficially, as one of *bulk reduction*. Thus, two approaches have been employed:

- The adoption of automatic deletion methodologies for all centrally stored e-mail messages, sometimes without regard to their status as records having retention requirements as established by the organization’s records retention schedules, and
- The establishment of limits on mailbox size and/or message age.

These management strategies are deficient in several respects; most notably, they ignore records management principles under which e-mail messages must be managed as records, based on their content and value, throughout their retention life cycle. A sample policy that incorporates these principles is shown in Figure 7-1. First, however, let’s take a look at the major technology infrastructure for managing e-mail in the U.S. and its deficiencies in applying records management principles to these messages.

In recent years, tools supplied by Microsoft® Corporation have become the predominant platform for managing e-mail. The major tools are Exchange, Microsoft’s groupware collaboration software, which typically resides on dedicated e-mail servers, and Outlook, the client e-mail software that manages individual mailboxes at the desktop level. In the MS Exchange environment, a user’s typical 45 megabyte (MB) allocation makes the mail folder at best a temporary repository—25 to 30 days worth of messages at an average of 1.7 MB per user per day. To free up space, users must either delete unneeded messages or migrate needed ones elsewhere, most often to folders residing on the desktop hard drive or to a network file server. Although the Microsoft Outlook client supports auto archiving old messages to personal message folders, unlike the MS Exchange message store, these messages are often not backed up. Moreover, the functionality that is installed in MS Exchange / Outlook software does not manage a full-scale retention plan. Nor does it have the “intelligence” to actually understand the content and context of an e-mail message to automatically determine whether it requires storage and if so where, and how to apply retention rules to govern its life cycle.

The very notion that an e-mail message can be easily destroyed is misleading if not erroneous. To the average user, destroying an e-mail message means deleting it. Deletion is one of the most poorly understood aspects of personal computing. When an E-mail message is deleted using the delete key, the act of erasure does not occur. This keyboard function merely signals the computer that the space required to store the message is no longer needed. The space is so marked, but the data that occupies it continues to exist until the computer overwrites it with new data. Thus, messages that users presume to have destroyed still, in all likelihood, reside on their desktop hard drives and are still retrievable.

The average e-mail message typically makes some 17 hops as it travels throughout various computing environments to arrive at its destination. E-mail messages are typically stored in the following locations:

- On the computer on which they are composed
- On the computer from which they are sent
- On the computer that receives them
- Often on any number of computers in between sender and receiver, especially if the messages are sent or received by external parties
- Finally, most large companies retain back-up tapes of e-mail backed up from their network servers.

From the foregoing, we conclude that no e-mail retention plan, however aggressively implemented, will be successful in eliminating all useless messages. This statement
does mean, however, that e-mail retention should not even be attempted. On the contrary, we strongly recommend e-mail retention, as indicated by the sample e-mail policy appearing in Figure 7-1.

Records Management Aspects of the Problem

From a records management perspective, the central issue is that e-mail systems were never intended to support the discipline of records management in which records are managed as records. Most e-mail systems presently do not offer the functional tools capable of providing any intelligence on e-mail content, because they are not “content-aware”; that is, they have no intelligence to understand the relevance of the data stored in them. They were never intended to support the need to manage and archive an organization’s huge volume of business data as long-term corporate assets. Moreover, many if not most users believe that e-mail is not a record, merely a means of communication. In fact, e-mail is just another form of a record. E-mail messages are or may become documents and records with the same legal requirements, restrictions, and standards as any other record produced in any form or medium.8

Without properly functioning electronic recordkeeping software, storing and maintaining e-mail messages as records for any significant period of time can be very difficult. As discussed in Chapter 8, although many organizations now use document management software systems, often little or no imbedded records retention functionality exists within them. However, placing electronic records into a controlled repository is critical for proper records management functions (i.e., filing standards, naming conventions, and retention periods) to be implemented.

Because of these factors, the management of e-mail is sometimes characterized as the single biggest records management problem in the USA. Thus, for any organization looking to implement major initiatives in the management of its electronic records, e-mail systems should be the initial focus of such efforts.

Legal Issues and Risks

Despite the fact that e-mail is one of the most efficient means of business communication ever invented, it is not without its risks. In fact, from a legal point of view, e-mail is probably the most legally risky form of business communication for the following reasons:

- E-mail users presume, incorrectly, that these messages are private in a similar sense as telephone communications. According to Erwin Chemerinsky, professor of law at the University of Southern California, “People should assume, especially in the work context, that what they write in e-mail is going to be seen.”9
- The nature of e-mail, as a communications medium, encourages chatty, informal modes of expression—very legally risky! According to Nancy Lasater, an attorney specializing in employment litigation in Washington, DC, “If I’m the plaintiff’s counsel, one of the things I want for sure . . . is the e-mail trail because that’s where the slips of the tongue and the slips of the fingers happen.”10

These issues found their most prominent expression in the recent Microsoft antitrust lawsuit. According to many legal observers, for Microsoft, e-mail made its antitrust defense more challenging than that ever faced by IBM, AT&T, or

---

**Figure 7–1 Sample Policy**

### MANAGEMENT AND RETENTION OF E-MAIL

**SCOPE / COVERAGE:** Company-wide — All E-mail Users

**General Principle:** ABC Corporation regards its e-mail systems as tools to facilitate daily communications of a transitory nature between employees and external parties relative to current business matters and not as a platform for the long-term preservation of official, mission-critical, or vital records. More specifically, ABC’s e-mail system is not authorized for purposes of the retention of stored records. The company desires to retain only such records as are needed to operate the business and comply with the law. All other records, including e-mail, should be systematically disposed of. Accordingly, the company imposes the following retention requirements on e-mail.

**Legal Status, Content, and Rights of Access**

ABC Corp. declares that all e-mail messages and attached documents are the property of the company and are therefore subject to reasonable management controls. E-mail is not
authorized for any purpose other than the conduct of official company business.

Employees are advised that they can make no presumption of any right of privacy with respect to e-mail. The company declares that it retains the right to access all e-mail files, just as it retains rights of access to any other company property. Finally, employees are advised that, from a legal point of view, e-mail messages are discoverable in litigation to the same extent as any other company information.

All e-mail must be as formal and businesslike as the situation dictates. Employees should construct the content of every e-mail message with the same care as if it were a paper letter or memorandum. The inclusion of remarks of a derogatory nature is strictly prohibited. Employees who violate these principles are subject to disciplinary action, up to and including dismissal.

E-mail Retention Policy

Except as provided below, the maximum retention period for e-mail shall be 30 days [alternatively 60 or 90 days] after the message is opened / read by its recipient, but employees are encouraged to delete the messages DAILY, immediately after reading, replying, or taking other action concerning them. Such actions are required of all employees during Records Review Days. This policy applies to documents attached to e-mail messages as well as to the messages themselves. Employees who fail to abide by this policy are subject to disciplinary action by the company, up to and including dismissal.

All opened e-mail older than 30 days [alternatively 60 or 90 days] remaining in employees’ mailboxes will be automatically purged upon the expiration of this retention period. The retention of e-mail data on back-up media will not exceed 30 days [alternatively 60 or 90 days].

E-mail of Long-Term Value

If the content of an e-mail message (or a document(s) attached to said message) possesses business value for longer than 30 days [alternatively 60 or 90 days] and relates to an established records series appearing in the Records Retention Schedules, it should be made a part of that established file and retained appropriately as per the retention period in the schedules. In such cases, employees are required to:

- Generate a hard copy printout and place it into the proper paper file for further retention in accordance with the Records Retention Schedules; or
- Migrate the message (and/or attached documents) from the e-mail system to another software program (e.g., in the MS Office suite or to a production application), if available, and save it for the retention period specified in the Records Retention Schedules.

These provisions should not, however, be construed to provide general authority to apply long-term retention to e-mail messages. The company desires to retain e-mail only if it is required to operate the business and comply with the law.

E-mail Related to Litigation or Government Investigation

If the content of an e-mail message is related to actual or pending litigation or a government investigation, it may not be destroyed without the expressed written approval of the Legal Department. This restriction begins from the moment at which any employee gains knowledge that litigation or a government investigation is imminently foreseeable (even though the lawsuit or investigation has not yet officially commenced) and continues until removed by the Legal
Standard Oil. An article in InfoWorld summarized the matter thusly: “Given the way the Justice Department used Microsoft’s internal e-mail documents to cement [its case], it’s time for companies to clean up their e-mail content and [retention policies] . . . Companies should not use e-mail as if it were ‘hallway’ conversations. If your culture condones these communications, you should determine appropriate e-mail retention policies.”11 For its part, Microsoft’s Nina Bondarook conceded the problem: “E-mail discovery has got everybody really scrambling.”12 The conclusion, of course, is that what is needed are viable and workable solutions to mitigate the legal risks associated with e-mail.

Retention Issues

Many organizations estimate that up to 70 percent of the e-mail data they currently receive does not possess long-term value and could be eliminated prior to archiving under a proper retention plan. The remaining 30 percent of the e-mail data contains information of long-term value—critical business information that is difficult to search, retrieve, and leverage for competitive advantage or litigation protection.13

However, all this e-mail data requires proper message categorization and retention management. E-mail retention practices range from the two extremes—draconian policies that require purging after 30, 50, or 90 days—to saving all or nearly all indefinitely. Some policies require users to print paper copies for ongoing retention. However, such policies may not be legally sufficient because printed copies of e-mails may not provide enough tracking or metadata, without which the record may be taken out of context.

The decision in Armstrong vs. the Executive Office of the President determined that, for federal agencies, retained e-mail messages must include the text of the message, the transmission data (minimally the identity of the sender and all recipients, and the date of transmission), and any attachments. The court held that not only the message but also related contextual information must be retained to ensure the message is understandable. Thus, the question of what must be retained and how it will be retained can often pose more difficult issues than the retention period itself.14

With respect to retention, ARMA International’s Guideline for Managing E-mail emphasizes that retention periods for e-mail records must be based on the content and value of the information contained in the messages themselves. Based on classic records management principles, e-mail may be characterized as a record type, but it is not a records series. This view supports the notion that no single retention period can be applied to all e-mail.15

Solutions

Today’s knowledge workers need to be given the tools to search, retrieve, and manage the life cycle of e-mail within a secure environment that allows true collaboration between all. One major problem is that, because e-mail technology is so new, the research on its usage and management is still in its infancy. Moreover, commercial software products targeted to the management of e-mail have been slow to develop. In particular, products to automatically classify e-mail messages to facilitate their retrieval and retention and disposition are in their infancy. However, new technology tools are now being introduced with the capability of understanding the content and context of the data residing in e-mail systems. These tools are being designed to support life cycle management of messages and their content, attachments, and accompanying metadata. Within several years, products that apply enterprise-level records management tools that categorize and manage e-mail messages throughout their life cycle, including e-mail that must be retained indefinitely / permanently as archival records, will be introduced.16

The ARMA Guideline for Managing E-mail explains what organizations must do to ensure that information contained in E-mail is properly managed in accordance with professional records management principles and practices.17 In the U.S. Department of Defense standard for records management software applications (DoD 5015.2-STD), mandatory requirements for these solutions include functionality for users to file e-mail messages and treat them as records. The standard states: “[Records Management Applications] shall treat e-mail messages the same as any other record, and these shall be subject to all requirements of this Standard . . . RMAs shall capture and automatically store the transmission and receipt data . . . if available from the e-mail system, as part of the record metadata when an e-mail message is filed as a record.”18

Management Issues

Based on the foregoing information, what are the management issues to be addressed in a new corporate policy for e-mail?19 We recommend the following management principles:

- General principle: The purpose of e-mail is to facilitate daily communications, not to provide an archival repository for the long-term retention of messages.
- Restrictions on message content
- Monitoring of e-mail usage / message content by management
- Establishment of retention policy / procedures
- Implementation of auto-delete functionality
- Implementation of message migration functionality
- Application of retention policy to data back-up systems
- Limitation of mailbox storage capacity
- Employee awareness and training

These management principles are embodied in the sample policy appearing in Figure 7-1. ABC Corporation is the fic-
CASE STUDY: E-MAIL MANAGEMENT AT ABC CORPORATION

General Observations

Most persons we interviewed had the opinion that management and retention of e-mail constitutes one of the single biggest records management problems at ABC Corp. In brief, for all its benefits, many persons believe that e-mail is now inadequately controlled at ABC, to the point where new management initiatives are needed. At its best, e-mail enables any enterprise such as ABC to conduct business in an efficient manner. At its worst, in cases where it is abused, e-mail can create a dysfunctional work environment, as well as major exposure to litigation risks in businesses such as ABC. Therefore, an e-mail management policy is required to address these issues and mitigate these risks.

Behavior Patterns

Behavior patterns regarding e-mail usage at ABC vary widely. Some users regard e-mail as a platform for daily communications only; they do not attempt to use it as an archival repository for old, inactive messages. These users tend to handle all their e-mail each day; they print messages having long-term value and delete the electronic versions immediately after reading / acting on them, and they tend not to establish folders as repositories for their e-mail in the Outlook environment.

At the other end of the continuum, a small but increasing number of e-mail users at ABC have come to regard e-mail and associated software in the MS Office suite as their sole recordkeeping system. Indeed, for some users, the large majority of their business (at least the portion involving written communications) occurs on e-mail. These advanced e-mail users tend to save many or most messages, either in folders established on the Outlook application, or on their C drive, or on one of the company’s network servers. Many of these users tend not to print messages for filing in paper files, considering this practice an old-fashioned way of going about their work.

Some e-mail users at ABC may receive literally dozens of messages on any given day (see survey data below); obviously, the effective management of this quantity of electronic documents consumes a significant portion of their workday. Indeed, some e-mail users retain hundreds or even thousands of e-mail messages indefinitely, never deleting any of them. Finally, most e-mail users at ABC fall somewhere between these two extremes with respect to how far they have progressed in the transition from paper-based to an all digital recordkeeping environment.

Policies / Procedures

At present, management has not attempted to impose any stringent retention policy as one means of managing e-mail. Nor has management attempted to incorporate auto-delete functionality as a means of managing e-mail. This functionality results in the automatic deletion of all opened / read e-mail messages after a specified period of time, which is expressed in the retention policy.

Technology Tools

ABC Corp. uses Microsoft Outlook on Exchange servers as its e-mail platform. The company operates at least 250 remote e-mail servers.

We confirmed that auto-delete functionality can be incorporated into the e-mail system. According to IT personnel, in the Microsoft Exchange / Outlook environment, automatically deleting opened messages after a specified period of time is technically feasible. The software can distinguish between opened and unopened messages for purposes of applying a retention period. This auto-delete functionality can be implemented either company-wide or at the individual mailbox level.

Utilizing the Clean Mailbox utility in MS Exchange, the IT Department can manually run a utility that will delete all e-mail older than a specified number of days. This e-mail purge can occur either after the date of receipt or after the last modified date of the messages. This utility can be applied to read items only, to unread items only, or to both read and unread items. Further, the Clean Mailbox utility can delete the items immediately, or move them to a “deleted items” folder for subsequent deletion. Finally, the Clean Mailbox utility can be applied to calendar and other items in the e-mail environment, as well as to the messages themselves.

The Clean Mailbox utility does not, however, extend to personal folders that have been established in Outlook. Thus, users who wish to retain e-mail messages beyond 90 days have the option of saving them to a personal folder in Outlook, or saving them out of the e-mail environment on their hard drive or on a common network server.

NOTES

1 “E-mail @ 30,” Computerworld, 12 November 2001. Although others were involved in inventing e-mail as
we know it today, Tomlinson (a computer specialist with the firm Bolt, Beranek, and Newman) is the undisputed source for the now ubiquitous @ symbol that separates the user name from the computer name and to indicate that the address is outside the network.

2 Ibid.

3 See, for example, Tony Kontzer, “More Than an Inbox: E-mail is Moving to a Broader Business Purpose,” Informationweek, 6 May 2002; Tim Shinkle, “Time for a New Look at E-mail Management,” Computer Technology Review, June 2001.

4 Ibid., “E-mail @ 30.”

5 Ibid., “E-mail @ 30.”; Ibid., “Time for a New Look at E-mail Management.”; Tim Shinkle, “Changing Technology Requires a New Look at Enterprise E-mail Management,” Storage Management Solutions 6, no. 3 (2001); Marcia Stepanek and Steve Hamm, “When the Devil is in the E-mails,” Business Week, 8 June 1998; Dean Foust, “The Check is in the E-mail,” Business Week, 30 October 2000.

6 Ibid., “Changing Technology Requires a New Look at Enterprise E-mail Management.”


8 See Bisher Abaza, “Managing E-mail Content: Challenges and Benefits,” KMWorld, May 2001; Ibid., “Changing Technology Requires a New Look at Enterprise E-mail Management.”; See also John T. Phillips, “Start with E-mail!,” The Information Management Journal 35, no. 4 (October 2001): 56–58; and Dan Schneider, “E-mail: Just Another Record,” e-doc, March / April 2001.


12 Ibid., “When the Devil is in the E-mails.”

13 Ibid., “Changing Technology Requires a New Look at Enterprise E-mail Management.”


17 Ibid., Guideline for Managing E-mail.


20 This case study was assembled from project work on various consulting engagements in which the authors have been engaged during the past several years. We are particularly indebted to Dr. William Saffady for developing the user survey data during the course of one such engagement.
One of the most important occurrences to affect recordkeeping and records management (RM) during the past twenty years has been the introduction of various technology solutions designed to enhance the management of records. This chapter addresses these solutions. We discuss several specific categories of these solutions, in the context of their contribution to managing the life cycle of electronic records through a retention methodology. We discuss the following three categories of solutions:

1. Records management software applications (RMAs), which evolved during the early to mid-1980s, for the purpose of bringing better management to paper-based recordkeeping systems;

2. Electronic document management software (EDMS), which evolved during the late 1980s and early 1990s, for the purpose of bringing better management to electronic documents created in PC-computing environments; and

3. Electronic document imaging software, which was introduced during the early to mid-1980s, for the purpose of replacing paper and microfilm-based recordkeeping systems.

Anyone who aspires to bring better management to the life cycle of electronic records needs to have a solid understanding of these solutions and how to deploy them. Although each of these solutions evolved as a separate and distinct family of software serving its own market, during the past five or more years they have gradually converged, for the purpose of delivering more comprehensive and robust solutions to the general problems associated with managing records and documents in multimedia formats throughout an enterprise.

The records management family of software products developed around the concept of life cycle management and records retention as their core objective. This functionality was, however, largely absent from electronic imaging and electronic document management solutions. This lack was certainly true during the early stage of development of these products and, to some extent, it remains true today. Rather, greater accessibility of information was, and remains, the primary goal of these solutions, rather than life cycle management. Thus, from the point of view of electronic records retention, the goal is how to integrate life cycle management functionality into these solutions as they are deployed in specific recordkeeping situations.

**RECORDS MANAGEMENT SOFTWARE**

This type of software was developed for the purpose of indexing, tracking, and monitoring the location and retention status of paper-based records. These software products were initially developed to operate on personal computer platforms and are designed to provide various types and levels of computer control over a wide variety of records management functions. Most early implementations tended to be application-specific and scaled to the workgroup level. The newest generation of software is developed for enterprise deployments.

Prior to the development of this type of software, most organizations had little or no computer capability to track and monitor the existence and location of their physical records. Nor did they have any computer capability to manage the retention of these records during the several stages of their life cycle. Records management software was developed to provide a solution to this problem. Records management software can be applied to active records maintained in single filing stations, throughout a department or division, or throughout an entire enterprise. Further, these solutions can be applied to inactive records in storage facilities. Finally, many of these products combine active and inactive records management functionality into a single, integrated solution. When thus deployed, the system is capable of providing enterprise life cycle management over the organization’s records, regardless of location.

For physical records, the basic retention functionality in records management software products consists of the following capabilities:

- Supports the development of records retention schedules, including the entry of records inventory data, the inclusion of citations for statutory and regulatory retention requirements, and the maintenance of approved retention schedules in the database.

- Contains a legal research database of U.S. federal and state laws and regulations impacting the retention of the organization’s records.
• Stores and maintains the retention schedules in a database; supports the implementation of the schedule’s disposition and retention requirements by linkage of records series to stored records, with subsequent assignment of retention periods and destruction dates to all records managed by the system.

• Calculates the dates on which records are eligible for destruction and prints reports listing records whose retention periods have expired, based on the retention periods contained in the retention schedules, in order to secure management approval of the destruction.

• Places holds on records in cases where authority to dispose of them has been suspended as a result of litigation, audit, or other requirements issued by legal authority;

• Provides documentation for which records have been destroyed under the authority of the retention schedules.

During the mid- to late 1990s, records management software products began to be upgraded to provide functionality for the management of electronic records as well as physical ones. These products generally adopted one of three approaches to the management of electronic records. The specific approach adopted by vendors tends to vary according to the exact electronic record formats handled by the system, the methods of classifying records, assigning retention periods, capturing metadata, handling searches and revision control, and performing document destruction. These approaches are described as follows:

• **Retention metadata linked to stored records but in separate repositories.** This approach works by capturing metadata about electronic records at the time of their creation, along with the document types chosen by their creators. These data are stored in a records management database where the document types are matched against their corresponding retention classifications, and retention periods are then assigned by the software based on document type. The electronic records themselves are not stored in the RM database; rather, they are stored in their native applications. Although this approach enables the searcher to know of the existence and location of electronic records and when they will be eligible for destruction as scheduled, no direct interface exists between the records management metadata in the database and the electronic records themselves. Thus, no direct capability to delete or destroy the records in their storage repositories is available; deletion / destruction must be accomplished as a separate task.

• **RM software integrated with EDMS system.** Under this approach, records management metadata fields are added to the document profile screens of the EDMS. When document creators complete these fields, the resulting metadata is stored in the database of the records management software, while the remaining metadata is stored in the database of the EDMS system. The documents themselves are stored in the repository of the EDMS. Thus, the records management software is serving as an adjunct to the EDMS system.

• **Retention metadata and stored records in shared repository.** Under this approach, the electronic documents and their associated metadata are stored and managed together in their own database. Some solutions also store the original documents in their native formats in designated directories.

### The DoD Standard

In 1997, during the time period when records management software products were adding functionality for electronic records, the U.S. government issued the first-ever standard prescribing requirements pertaining to this matter. The standard is DoD 5015.2-STD, Design Criteria Standard for Electronic Records Management Software Applications, which was issued by the U.S. Department of Defense on November 24, 1997, and revised in 2000. The standard has been endorsed by the U.S. National Archives and Records Administration (NARA). According to some observers, it has (or soon will) become the de facto standard for the acquisition of records management software by state and local governments as well as by the private sector throughout the U.S. and perhaps abroad.

DoD 5015.2 is the first standard to establish detailed technical requirements for software that manages records in electronic form, and it is certain to have a significant impact on records management programs everywhere. A technical measurement tool for software products designed to manage records under a formal records management program is now available.

The standard differentiates between records and document management software but prescribes combined design criteria relevant to both classes of software intended to provide for the lawful management of electronic records as required by DoD and NARA regulations. The standard defines a document management application as a system used for managing documents that allows users to store, retrieve, and share them with security and version control. A records management application (RMA), on the other hand, is defined as software used by an organization to manage its records. The primary functions of an RMA are defined by the standard as categorizing and locating records and identifying those due for disposition as provided by an organization’s retention schedules. RMA software also stores, retrieves, and disposes of the electronic records stored in its repository. The standard requires compliant software to have the capability to view, copy, print, and if appropriate process any electronic records stored in the RMA for as long as those records must be retained.

The RMA Certification Testing page issued by the Joint Interoperability Test Command of the Defense Information Agency lists RMAs currently certified as being compliant.
with the standard. In the context of product functionality for records retention, the following generalizations may be made:

- All products require a file plan, derived from the retention schedule, to be built into the system.
- All products have the capability for managing electronic records in some sort of repository, as well as providing a means for managing paper as well as electronic records through record profiles.
- Most products store records in their original or native formats as binary objects together with descriptive metadata in a relational database.

The provisions of the DoD standard pertaining to records retention appear at the end of this chapter.

**ELECTRONIC DOCUMENT MANAGEMENT SOFTWARE**

The electronic document management systems (EDMS) category of software evolved in response to the PC revolution that brought computers to the desktops of office workers everywhere. As discussed in Chapter 6, during the early days of PCs, when the DOS operating system served as the predominant tool for managing electronic records created on PCs, the management of these records tended to be very primitive and rudimentary. Throughout the 1980s, whenever most PC users saved a document, they would assign a filename consisting of eight characters followed by a three-character extension. In many PC-computing environments, this brief and cryptic filename (known only to those who assigned it) tended to be the only management device applied to the mass of desktop documents throughout the organization. This situation obviously cried out for better management, and software vendors developed electronic document management software in response.

EDMS solutions are frequently integrated with other classes of document technologies in specific recordkeeping environments. These technologies include electronic document imaging, full-text retrieval, workflow, and others. Other technologies are also of high importance to the deployment of an EDMS. These technologies include database management systems (DBMS), groupware, and the **Internet** and its related technologies—the World Wide Web, browsers, intranets, and others.

EDMS systems are designed to capture, version, route, and organize corporate electronic documents in workgroups and on an enterprise-wide scale. These systems also provide collaboration, distribution, and secure access. EDMS solutions are based on the concept of a document repository. This term refers to the use of a database management system to store and access information associated with documents saved in and managed by the EDMS. The database contains index or profile information and other metadata.5

In most EDMS implementations, document creators are required to fill out what are called document profiles. These profiles are structured abstracts that must be completed for each indexable document to be managed by an EDMS system. The profiles contain index data describing the document in terms of subject keywords and other key descriptive elements. Typical profile fields include:

- filename
- title
- author(s)
- subject(s) or keywords
- date created
- audience
- version / date modified
- access restrictions / authorized viewers
- life cycle management data

**Solution Convergence**

Earlier, we noted that the primary purpose of EDMS software is to provide a solution for bringing better management to unstructured electronic documents created at the desktop level throughout an organization. This purpose raises the question as to where records management software solutions are going with respect to interfacing with EDMS software and in managing electronic records generally. Most EDMS software products lack the following critical records management capabilities:

- Some method of declaration—a mechanism to define whether an electronic document is an official record and thus requires management in accordance with the organization’s records management policies and procedures.
- The ability to perform formal retention and destruction of electronic documents, based on their classification and retention status as defined in the organization’s records retention schedules.
- The ability to track and control documents that are outside the system, including those that exist as paper documents.
- The ability to track the location of all records, regardless of format or media, so that they may be located and destroyed according to the appropriate records retention schedule.6

Records management applications can greatly enhance an organization’s information strategy when integrated with an EDMS system. A common enterprise strategy for document and records management should address classification and indexing (metadata models), repository design, life cycle management, and integration with the information technology infrastructure.

Some EDMS solution providers are currently beginning to integrate this records management functionality into their product lines. On the other hand, some records management software vendors have begun to integrate EDMS functionality into their product lines. In these
cases, the records management software will be able to handle records in electronic formats to enable the software to integrate with the native applications on which electronic documents are created or received—productivity tools such as word processors, spreadsheets, and e-mail systems. This type of integration will permit users to access the records management system from an interface other than the records management software itself, such as a Web browser, an EDMS application, or tools such as Microsoft Word or Lotus Notes.7

Records Retention Functionality in EDMS Solutions

For the most part, EDMS solutions were developed without significant input from the records management community. As a result, early products included little if any functionality for records retention or document life cycle management. Part of the problem is that records management specialists and document management software vendors often apply very different meanings to the term document life cycle. Records managers typically apply this term to mean the transition of a record from an active to a semiactive and finally to an inactive state. In document management parlance, on the other hand, the document life cycle often refers to the controls applied to a document through multiple editing, revisions, and versions to its issuance or publication.

Thus, through the mid- to late 1990s, most document management software packages provided little or no records retention functionality. A few products provided a field for retention periods in the document profile. With respect to life cycle management, the “date of last access” has traditionally been considered the prime factor determining whether a document should be kept on-line, near-line, or off-line. The last access date, however, does not govern whether or when the document has reached full retention and requires review for destruction. Thus, the majority of the early EDMS solutions tended to address the retention issue by simple metadata fields without an integrated methodology for implementing a formal records retention strategy.

Today the situation has improved substantially. Today’s EDMS products frequently do include a life cycle (retention) component, but these components are not as robust as records management applications, which are designed with life cycle management as one of their core objectives. Retention functionality in EDMS environments requires that the software be capable of classifying documents according to the records retention schedule, automatically attaching a retention period to documents based on the classification chosen, recognizing that retention may have to be calculated from a trigger event (for example, the expiration of a contract or permit). The following discussion details these matters.

Retention Policy Issues

Retention policy issues in EDMS environments include:

- What rights and privileges should end-users have in retention matters? Should all users have equal privileges in adding documents, editing them, and deleting or assigning retention periods to them?
- For purposes of applying retention rules, how should users distinguish between draft documents and final documents? What retention rules should govern these documents?
- Should documents receive a retention period at the time of creation? Should document creators be responsible for classifying documents for retention and for assigning retention periods? Can assignments be done automatically?
- What procedures will govern the disposition process when documents reach their full retention?8

Assigning Retention Periods

In integrating retention functionality into the EDMS, one of the following three approaches may be adopted in the assignment of retention periods.

1. They may be assigned from the database.
2. They may be user assignable.
3. They may be assigned based on rules associated with records series prefixes or document types.9

The most recent efforts to integrate retention functionality into EDMS solutions employs the workflow approach in which workflow rules are employed to assign the retention periods. The premise is that a known, controlled workflow process produces certain known classes of documents that may be classified based on the work steps of the process. Further, retention periods for these document classes would be based on the expiration of value of the documents in supporting their business processes.

Document Destruction

The scheduled destruction of electronic records in EDMS applications is just as important as it is in other record-keeping environments. Although individual documents can be deleted even by desktop applications, an EDMS solution should provide tools and safeguards to assure that this activity occurs responsibly and efficiently. Document management methods and practices can only be applied to documents created within or managed by the system itself.

EDMS systems should enable deleting documents singly by users or in bulk mode by system administrators. A period of undeletion should be available subsequent to which the document is completely ablated in order to assure that it cannot be reconstructed. Some volume deletions will need to be initiated automatically based on
retention periods or other available guidance or existing document metadata such as automatic last accessed date, index value, or document type. Document deletion must be auditable with appropriate notices generated when necessary and in compliance with overall enterprise records retention schedules. A more detailed discussion of retention functionality in software applications appears in Chapter 12.

**ELECTRONIC DOCUMENT IMAGING SYSTEMS**

As noted earlier, electronic document imaging solutions were introduced during the early to mid-1980s, primarily for the purpose of replacing paper and microfilm-based recordkeeping systems. These systems consist of configurations of various hardware / software components to record and retrieve digital documents and data on optical media or high-performance magnetic storage solutions. Documents and data are recorded onto optical media by means of a high concentration of laser light. Electronic document imaging systems were the first solutions specifically targeted to provide a replacement for paper-based document information systems since the 1920s when microfilm began to be used for business records. They were also the first-ever computer-based solutions. Their biggest benefit is high-speed retrieval with desktop display, particularly when compared to paper-based recordkeeping systems.

Because most imaging systems are designed with the primary goal of improving information accessibility, document life cycle management through a records retention methodology is frequently de-emphasized if not completely ignored. Few imaging solutions incorporate a well thought out, robust retention component.

**Nonerasable media**

In imaging systems utilizing nonerasable media, successfully executing a records retention methodology is very difficult. In these implementations, which utilize what are called WORM or write once, read many times optical media, once document images have been recorded onto the surface of the optical platters, they are permanently encoded; that is, they can be read repeatedly but never changed or erased. This form of imaging technology was designed to be an electronic replacement for microfilm—an appropriate solution in archival applications in which the documents are considered to be of evidentiary value. Thus, they require permanent capture in immutable form on the media on which they reside. Although executing a retention methodology by copying all documents residing on single platters requiring continuing retention onto new media and destroying the old media containing the images eligible for destruction would be theoretically possible, such a process would be very cumbersome and is, in fact, rarely attempted.

During the 1980s and early 1990s, some imaging specialists advocated the “virtual purge” as a means of executing a retention methodology in write-once imaging implementations. Under this methodology, the index pointers to document images would be erased or deleted when such images reach retention maturity, thereby rendering the images irretrievable in normal use. The images themselves would, however, continue to reside on the WORM platters. When the media is destroyed or current records are transferred to new media, the “deleted” records are not transferred, and the original media is removed from the system and physically destroyed.

From a legal point of view, however, this virtual purge methodology is problematic. For example, if document images are requested under subpoena and are still extant on storage media even though the index pointers have been deleted, the court could elect to enforce the subpoena by requiring the owner of the records to search for them regardless of how difficult this task may be. After all, this virtual purge is analogous to removing folder labels from files or carton labels from boxes, even though the folders and boxes are not, in fact, discarded. For these reasons, the virtual purge methodology cannot be recommended as a proper approach to incorporating a retention methodology into imaging environments.

**Rewritable Media**

Other imaging implementations employ erasable or rewritable media, which function in a manner similar to traditional “write-over” magnetic media. This media type is often employed as a solution for highly active documents in dynamic recordkeeping environments. Here, the system is capable of effecting the deletion of expired or superseded images, just as occurs in normal computer applications utilizing magnetic, write-over media. However, even when erasable media is used, a robust retention methodology is still difficult to implement because most systems lack the required functionality. Some vendors have configured systems in which images having the same retention period are stored on the same disks so that the entire disk can be destroyed when the retention period has expired. This approach, however, requires that the media be dedicated to storing records of a uniform type and subject to the same retention period. In these implementations, procedures would need to be put into place to optimize the media by defragmenting routines.10

**CONCLUSION**

Records managers should consider carefully the requirements concerning document disposition, retention, and other life cycle management issues during the initial planning and design of any software solution. Any required functionality should be incorporated into the design and configuration of the solution prior to its implementation.
Otherwise, such functionality must be retrofitted later. In cases where the required retention functionality has not been incorporated by vendors supplying commercial, off-the-shelf software products, records management specialists should work with applications developers from IT departments as well as vendor personnel to integrate such functionality as soon as possible. Chapter 12 contains a sample policy that addresses this matter.

**RECORDS RETENTION REQUIREMENTS SPECIFIED IN DoD 5015.2-STD**

The following requirements pertaining to the retention of electronic records appear in the Design Criteria Standard for Electronic Records Management Software Applications, DoD 5015.2-STD. These requirements are mandatory for vendor software products in order to achieve compliance with the standard. The following material was extracted verbatim from the standard. The full text of the standard appears in the Appendix.

**Scheduling Records.**

RMAs shall provide the capability for only authorized individuals to view, create, edit, and delete disposition schedule components of record categories. RMAs shall provide the capability for defining multiple phases (e.g., transfer to inactive on-site storage, transfer to off-site storage) within a disposition schedule.

RMAs shall provide the capability for only authorized individuals to define the cutoff criteria and, for each life cycle phase, the following disposition components for a record category:

- Retention Period (e.g., fiscal year).
- Disposition Action (interim transfer, accession, permanent, or destroy).
- Interim Transfer or Accession Location (if applicable).
- RMAs shall, as a minimum, be capable of scheduling and rescheduling each of the following three types of cutoff and disposition instructions.

  **Time Dispositions**, where records are eligible for disposition immediately after the conclusion of a fixed period of time following user-defined cutoff (e.g., days, months, years).

  **Event Dispositions**, where records are eligible for disposition immediately after a specified event takes place (i.e., event acts as cutoff and there is no retention period).

  **Time-Event Dispositions**, where the timed retention periods are triggered after a specified event takes place (i.e., event makes the record folder eligible for closing and/or cutoff and there is a retention period).

RMAs shall provide the capability to automatically calculate the complete life cycle, including intermediate phases, of record folders and records not in folders.

RMAs shall provide the capability for rescheduling dispositions of record folders and/or records (those not in folders) during any phase of their life cycle if an authorized individual changes the disposition instructions. This requirement includes the capability to change the cutoff criteria of disposition instructions and to change the retention period associated with a disposition.

The RMA shall provide recalculation of the record life cycle based on changes to any life-cycle date and set the filing status (i.e., open, closed) of the folder according to the business rules associated with date change(s).

**Destroying Records.**
RMAs shall identify and present the record folders and records, including record metadata, that are eligible for destruction, as a result of reaching that phase in their life cycle. Records assigned more than one disposition must be retained and linked to the Record Folder (Category) with the longest retention period. Links to Record Folders (Categories) with shorter retention periods should be removed as they become due.

RMAs shall, for records approved for destruction, present a second confirmation requiring authorized individuals to confirm the delete command, before the destruction operation is executed.

RMAs shall delete electronic records approved for destruction in a manner such that the records cannot be physically reconstructed.

RMAs shall provide an option allowing the organization to select whether to retain or delete

NOTES


2 Ibid.


9 Ibid.


11 Ibid., DoD 5015.2-STD.
During the past several years, virtually all U.S. businesses and other organizations have moved aggressively to reinvent their business processes around new information technology. One such technology is corporate intranets, which are a deployment of standard Internet technologies designed to provide common, consistent, and global access to various forms of information to employees. Most organizations view this technology as key to achieving their strategic business objectives. Many organizations have embraced a strategic direction for the Web that may be summarized as follows:

The company anticipates that its intranet and the Web sites that comprise it will become the primary method for the deployment of e-business solutions and for accessing stored electronic information enterprise-wide. Thus, developing common policies and practices for managing information in Web environments on an enterprise-wide scale is imperative.

In almost all organizations with which we are familiar, records retention / life cycle management issues have been neglected or ignored entirely where the Web is concerned. This chapter addresses records retention for the Web.

An intranet is a private network inside a company or organization that uses the same software as the public Internet but is restricted to internal use only. A typical intranet consists of one or more intranet servers. These servers are powerful shared computers that store the various documents and data that comprise the content. These documents share a common address—the universal resource locator (URL).

Users access the servers with Web browser client applications such as Microsoft Internet Explorer or Netscape Communicator. The documents on the intranet are stored in hypertext markup language (HTML) format, which allows for hypertext links, or pointers in documents that transport the user to a second document referenced by the pointer. These documents are, in fact, organizational property and should thus be managed as records under appropriate records management and retention policies and practices.

Because intranets are developed utilizing several technology toolsets (i.e., Web document authoring tools, proprietary server technologies, and specialized programming languages), most lack any real records management or retention functionality. More specifically, intranets have no inherent means of applying a retention policy to effect the scheduled disposal of the electronic documents residing in them. The guidelines recommended in the next sections are designed to rectify this need.

APPLYING RETENTION TO WEB SITES

In many implementations, intranet documents are frequently updated, with new documents replacing the superseded ones. Replacement destroys the provenance of the records as well as the capability to preserve a revision history of the documents throughout their life cycle. Documents may be removed from Web sites for many reasons, including:

- They no longer reflect current policy.
- The information in them has been superseded.
- Hard copies have been generated for retention / preservation.
- Official copies exist elsewhere.

Few Web authoring tools provide version management capabilities similar to those found in EDMS solutions. Each document, however, should have the appropriate retention applied to it. Retention periods can be added by classifying the document against the organization’s file plan and retention schedule. The Webmaster assigned to administer each site should assume the responsibility for performing this task, which should generally be done when the documents are initially uploaded to the Web server.

Web sites and their content may be static or dynamic in character. Static sites consist simply of static documents residing in folders on Web servers, tied together with hyperlinks. Dynamic sites, on the other hand, consist of content generated “on the fly”; that is, the component parts of individual pages—their content, structure, and presentation—are assembled based on specific user instructions at a given point in time. Different archiving and retention strategies will be needed for both types of sites.

Basic Web site information usually exists in multiple copies. These copies include the original paper source documents, the Web pages on the Webmaster’s PC, and the published version on the Web server. Basic intranet
contents are similar in that they consist of duplicates of paper documents, with the published version residing on the Web server. From a records management perspective, intranets and Web sites contain records that should be managed utilizing similar principles as are employed for any other paper or electronic information. These principles include retention or life cycle management concepts. Thus, the content of Web sites and intranets need to be scheduled for retention.

**PRESERVATION OF WEB CONTENT**

Nathan Myhrvold, former Chief Technology Officer at Microsoft Corporation, sent an electronic “Save the Web” message to a group of his colleagues. “The Internet isn’t naturally archival,” he said. “The Net isn’t going to archive itself.” Although this comment addresses the preservation of content on the World Wide Web as opposed to organizational intranets, Mr. Myhrvold’s point is nevertheless well taken. Web servers are not records management systems or long-term repositories; rather, they are designed to provide convenient access to information. Unless an organization has implemented a policy to maintain an electronic record in its native format for migration and functional management purposes, only the HTML format or a format such as the portable document format (PDF) is retained. Where required, organizations should consider strategies for transferring original electronic records with their associated metadata / tags to a long-term repository for continuing utilization, preservation, and management, according to approved retention policies.

For intranet documents appraised as possessing long-term or permanent value, copies of the documents, together with appropriate metadata, may be archived within a secure repository separate from the Web server itself. These documents should then be subjected to the preservation practices discussed next. In cases where Web sites contain historical information scheduled for long-term or permanent retention, the PDF format provides the most effective way of effecting such preservation. When using a Web browser to print documents, frequently items do not all fit onto one page, and some graphic or frame content does not print. By saving the content as PDF files, this problem can be greatly reduced if not eliminated. Once converted to PDF, the content may be properly printed and stored in paper form or microfilmed for permanent preservation in that format. For a further discussion of the role of PDF as a tool for long-term document retention, see Chapter 11.

Finally, Microsoft Corporation is building extensible markup language (XML) into all its products and systems; XML is open (nonproprietary), and it is certain to become a de facto global standard for metadata. It supports preservation and content of electronic information. For these reasons, XML should play a major role in the management of electronic records in Web sites.

**Figure 9–1 Sample Policy**

---

**THE RETENTION OF WEB PAGES**

Like other recorded information created and maintained by employees, Web pages created for an ABC’s intranet are records and should be managed as such. They document the mission, organizational status, policies, practices, and other key aspects of ABC’s business. As such, Web pages on the Intranet should be subject to ABC’s Records Retention Schedules, which apply to recorded information in all formats.

Records retention issues should be considered whenever Web pages are planned, created, or modified. Creators of Web pages should be responsible for determining retention periods for specific pages in conformity with ABC’s Records Retention Schedules and with the advice and consent of the Records Management Department. Intranet site administrators should be responsible for ensuring that retention periods are implemented through deletion or archiving of Web pages as discussed in the following sections.

**Basic Concepts**

As with other corporate records, retention of Web pages is based on their content and business value, but significant differences exist between Web pages and other types of records, including other electronic records. These differences can have an impact on retention decisions. In particular:

- Web pages may vary in purpose. Some contain recorded information; others serve as por-
or front-ends to other information such as documents or databases.

- Some Web pages are subject to frequent revision. The dynamic content of Web pages makes version control critical and raises questions about retention of superceded information.
- Given the interrelationships among Web pages on an intranet site, changes to any given page can have a ripple effect throughout the site. In particular, modification or deletion of one or more pages can adversely impact site navigation.
- Given the elaborate formatting characteristics of many Web pages, archiving of printed copies may not fully preserve content or functionality.
- Links to other sites on ABC’s intranet or the public Internet can complicate archiving of Web pages. Although a Web page itself can be archived, linked sites may change or disappear over time.
- Retention determinations for Web pages depend on their relationship to other company records:
  - A Web page may contain unique information not available in other company documents or databases.
  - A Web page may replicate information available in other company documents or databases, but the page may employ a distinctive presentation format or have other attributes with informational or evidentiary value.
  - A Web page may replicate information available in other company documents or databases and have no distinctive attributes with informational or evidentiary value.

Specific Retention Guidelines

All Web pages on ABC’s intranet must be dated to indicate when the page was initially created (activated), when it was last modified, and when it was last reviewed for retention.

Creators of Web pages for ABC’s intranet should determine retention requirements at the time Web pages are planned. The Records Retention Schedules should be consulted to determine appropriate retention periods based on the content and business value of information contained in specific Web pages. The Records Management Department should be contacted for clarifications or other assistance as necessary. Retention requirements should be re-evaluated whenever Web pages are modified.

Web Pages as Official Records

If a Web page contains information created specifically and exclusively for ABC’s intranet and if that information is not replicated in other documents or databases, the Web page should be considered an original record and treated as an official copy for retention purposes.

- If the records retention schedules specify a retention period for the type of information the Web page contains, that retention period applies to the Web page.
- If the records retention schedules do not specify a retention period for the type of information the Web page contains, the Web page creator should contact the Records Management Department for retention advice and assistance.

If a Web page contains information that is replicated in other company documents or databases but has distinctive attributes with informational or evidentiary value, the Web page should be considered an original record and an official copy subject to the retention practice...
Web Pages as Duplicate (Nonofficial) Records

If a Web page contains information that is replicated in other company documents or databases but has no distinctive attributes with informational or evidentiary value, the Web page should be considered a convenience copy—nonofficial in character—and treated like any other duplicate record for retention purposes.

- If a retention period has been determined for the type of information the Web page contains, the Web page can be retained up to that period of time, but it may be discarded at an earlier time if no longer needed.
- If ABC’s Records Retention Schedules do not specify a retention period for the type of information the Web page contains, the Web page creator should contact the Records Management Department for retention advice and assistance.

Deleting Web Pages

NOTES

1. For a good, general discussion of corporate intranets, see Bruce Miller, “Surfing the Issues of Corporate Intranets,” InfoPro 1, no. 4 (December 1999): 34–39.


5. This sample policy was assembled from project work on various consulting engagements in which the authors have participated during the past several years. We are particularly indebted to Dr. William Saffady for developing the data retention elements of this policy during the course of one such engagement.
What if . . .

- The Dead Sea Scrolls—the oldest extant manuscript copies of any books of the Bible—had been recorded on floppy disks instead of leather . . .
- The text chiseled on the Rosetta Stone, without which the recorded history of ancient Egypt would still be Greek to us, had instead been created on a word processor . . .
- Thomas Jefferson had saved his drafts of the Declaration of Independence on the hard drive of his laptop computer . . .

. . . Would any of these stupendous creations still exist today?

As you reflect on this question, remember that the greatness of many literary and artistic achievements are not recognized until many years after their creation—periods of time frequently exceeding the service lives of hardware, software, and storage media on which digital data reside and without which such data is unusable and, literally, consigned to the dustbin of history!

Edith Allen, manager of records operations at the Battelle Memorial Institute, reports: “Our in-house computer staff tells us that they can provide storage for 3 to 5 years with certainty; 7 to 10 years with a ‘little bit of luck;’ and if storage is required after 10 years, there are no guarantees.”¹ Battelle is a highly sophisticated scientific institution having, presumably, an equally sophisticated computing infrastructure. In the same vein, Jeff Rothenberg, senior research scientist at the RAND Corporation offers the somewhat whimsical observation that “digital documents last forever—or five years, whichever comes first.”² As with most such utterances, these two resonate because they have more than a grain of truth to them.

The problem of long-term data retention (or digital preservation, as we frequently refer to it here) is by no means confined to the computing environments of the U.S. A couple of years ago, we received an e-mail from Reykjavik, Iceland, that read as follows:

At my archives we are now receiving information in digital form almost every week. In endless sizes and formats. Up to 15 to 20 years old. Most of it is impossible to read today and some of it has permanent value, but it is not available on paper, so it is really lost. It is a great and GRAVE problem. How we can be sure to preserve our information today for the future. But this is not a problem for the future but for today.³

For an example closer to home, consider the irony in this little story: This author wrote a chapter on archives management for Information and Records Management, Fourth Edition, published by Glencoe in 1995. He wrote this chapter and five others during 1993-94, using a 386 PC with WordPerfect 5.1 for DOS software. However, in 1996, when the author upgraded his desktop technology to a Pentium-class machine with Microsoft Windows operating and applications software, he did not migrate the chapters to this new platform. He was just too busy to make document migration a priority. The result: In computer-processible form, the chapter on archives management has been consigned to oblivion. The written word, however, endures; copies of the book reside securely in libraries throughout North America. The moral of this story: The electronic version of this record lasted less than ten years; the paper copies should remain usable for many hundreds of years.

As the preceding examples illustrate, the essence of the digital preservation problem can be stated succinctly as follows:

If an organization creates a record in electronic format in, say, the year 2001, and this record will need to be digitally processed and read many years later, how, exactly, can this requirement be supported?

This chapter and Chapter 11 address this vexing question.

In this chapter, we acquaint the reader with an understanding of the pervasiveness and degree of severity of the digital preservation problem. We also highlight some potential solutions just now appearing on the scene. Chapter 11 is devoted to the current state-of-the-art in best practices for long-term data retention.

**DIGITAL PRESERVATION IS MUCH MORE DIFFICULT**

The digital preservation problem, in order of magnitude, is greater than the problems associated with preserving physical records. With physical records, the information is contained on media that is relatively durable or extremely so. Moreover, these records can be read by sight or, in the
case of microfilm, with the aid of relatively simple viewing devices. With physical records, deterioration is generally visibly apparent and a window of time is available—usually measured in years if not decades—during which conservation measures may be undertaken if required. From a technical point of view, nothing is particularly complex about preserving physical records for decades or even centuries. Once such records are appraised as possessing permanent retention value, they must simply be housed in environmentally appropriate space. When thus stored, the records should retain their integrity/usability for many decades if not for hundreds of years.

With electronic records, however, the situation is drastically different! These records are recorded on nondurable media, they are not human-readable, and the hardware and software required to read them is even less durable than the media on which the records have been recorded! Moreover, unlike physical records, digital records do not—indeed they cannot—survive by accident. The only way digital data can survive is by design; that is, by a series of carefully planned and executed tasks. These tasks are technically difficult, and specialized expertise as well as the requisite hardware, software, and systems documentation are required. These tasks can be quite expensive, and they must be performed periodically for as long as ongoing retention is required.

**No Ideal Solution**

The crux of the matter is that no one in the world has yet produced a way to preserve electronic records permanently. More precisely, no ideal solution to the problem of preserving electronic records is available today. An “ideal” solution would be “once-and-done”; that is, it would not need to be repeated over time. Moreover, it would represent a “proven solution” to the problems of hardware and software obsolescence and media stability. However, no such solution exists in the world today. Even such working models for digital preservation as are available today (e.g., the Division for Electronic and Special Media Records Services, U.S. National Archives) may be characterized as experimental in the sense that they are relatively small scale, their ability to scale to mass storage systems across the entire U.S. Government is unproven, and they are based on best practices that must be repeated every time data formats, hardware and software paradigms, or recordkeeping practices change. A discussion of this division of the National Archives appears at the end of this chapter.

However, organizations do not have the luxury of doing nothing while they wait for such a solution to appear on the horizon. Electronic records of long-term value are getting older by the day, and they may be threatened with attacks on their integrity/processibility or even abandoned by their owners. For these reasons, organizations must have a plan for how to deal with this situation, and they must implement this plan as aggressively as possible.

**An Unprecedented Challenge**

In 1996, the Commission on Preservation and Access and the Research Libraries Group issued the final report of the Task Force on the Archiving of Digital Information. The conclusion was alarming: “There is, at present, no way to guarantee the preservation of digital information; that is, there is no viable long-term strategy to ensure that digital information will be readable in the future. [This places at risk] this generation’s knowledge into the future.”

This situation is unprecedented in all of recorded history. As noted previously, in a preservation context, computer technology and the digital data that results from it are dramatically different from anything that preceded it. The reason is that computer data storage media have no qualities of durability, no “permanent keeping properties” in the traditional meaning of this phrase!

For the past 5,000 years, various civilizations have used baked clay tablets, papyrus, parchment, paper, and microfilm as media for recording information. Each of these media possessed adequate to excellent properties to support long-term preservation requirements. However, never has any society utilized any technology for recording, storing, and reading information that inherently lacked any real properties of durability.

What percentage of electronic records will or may require permanent preservation in computer-processible form? Probably less than 5 percent, but several trends suggest that this small amount may increase substantially in the future. The following major trends are spurring the growth of computer data of long-term value.

- The explosion in the growth of electronic records.
- The shift from paper-based to paperless recordkeeping systems, coupled with the fact that most if not all recordkeeping systems of high strategic importance have been converted from paper to digital format, many of which have long-term retention requirements.
- The fact that some large electronic collections of records exist solely in electronic form and are not usable in any form other than digital.

The conclusion: Most large organizations, and many smaller ones, will have to address the problem of how to support multidecade or permanent retention of digital data at some point in the future.

**Pervasiveness of the Digital Preservation Problem**

Countless examples of valuable digital records that need to be preserved can be found around the world. Unfortunately, sometimes plans for their preservation are not available. Here are five such examples:

1. The Boeing 777 commercial jet airplane was designed in a largely paperless environment. Thus, thousands
of engineering drawings, specifications, calculations, and dozens of other records—all in electronic form—were created. Most of these records must be retained for a retention period equal to or greater than the service life of the aircraft—at least 30 to 40 years. Retaining this large amount of records will require a major digital preservation effort at this company.

2. Today, virtually all new music, animated art, and most literature and academic works are created and stored in computers. Society has traditionally presumed that most such creative works possess enduring value. However, no organized and comprehensive preservation initiatives are in place to provide for their preservation.

3. Several years ago, scientists from the Jet Propulsion Laboratory, Pasadena, California (a part of the U.S. National Aeronautics and Space Administration), tried to read some of the magnetic tapes that contained the results of the 1976 Viking mission to Mars—tapes that had been carefully stored and appeared to be in good condition. However, they found that 10 to 20 percent of them had missing data. Consider this hypothetical analogy: An archive or museum in Spain or Portugal has custody over the priceless journals of Christopher Columbus, Ferdinand Magellan, or other explorers of the fifteenth and sixteenth centuries, and permitted them to deteriorate! Any archival institution that allowed this deterioration to happen would surely be accused of professional malpractice. However, the Jet Propulsion Laboratory did essentially the same thing.

4. Maxus Energy, a petroleum firm, maintains some 20,000 magnetic tapes containing seismic data, which is generally scheduled for permanent retention, stored in a warehouse in Houston. However, the company has no maintenance and inspection program for the records and their preservation status is not known.

5. Satellite photos of the Brazilian Amazon taken during the 1970s—data critical to establishing deforestation trends both regionally and globally, are reportedly stored on unreadable magnetic tapes.5

Accepting Responsibility for Digital Preservation

Beginning with the 2000 Federal Census, the U.S. Bureau of the Census has stated that it will not transfer the digital images of original census forms to microfilm. Let’s consider the preservation implications of this decision. With the 2000 census, the Census Bureau is, for the first time, making digital images of the questionnaires—the forms filled out by enumerators and individual citizens. Computers read the images and translated them into digital format. The 1970 census was the first in which questionnaires were mailed to homes and filled out by individuals. Moreover, the 2000 census might be the last one in which these source documents are filled out by hand. Some 70,000 of these forms were filed electronically in the 2000 census, and this number is expected to increase dramatically in 2010. However, officials with the U.S. National Archives and Records Administration, which has statutory responsibility to preserve the nation’s historical records, have stated publicly that the National Archives cannot handle these source documents in digital format. Consequently, for the first time, the Archives plans to retain just the master electronic files containing the census data and none of the images that show actual handwriting or other information content appearing on the paper questionnaires.

The Census Bureau, for its part, states that its mission is to collect, store, and analyze data, not preserve documents. Nevertheless, it has agreed to maintain 4,640 tape cartridges that contain the digital images for the 1990 census. However, if the National Archives does not take eventually them, the Bureau indicates they will be destroyed.6

Thus, we see the all too common dilemma of digital preservation: Who accepts responsibility? More to the point, who pays? The creator and original owner, who has little if any incentive and perhaps little if any capabilities and resources? Or some separate archival repository that is in the digital preservation business but may not have adequate resources to do what is required on a permanent basis? Our society is just now in the early stages of addressing these issues. Anything approaching viable solutions is a long ways away.

The Most Severe Manifestation

As was noted in Chapter 2, our ability to produce data is rapidly outstripping our ability to manage and preserve data. The Age of the Petabyte is upon us. Analysts from Gartner, Inc., predict that, during the next several years, database sizes will approach 1,000 terabytes, or one petabyte.7 During the past 10 years, the growth of digital data in mass storage systems has outpaced data transfer speeds by a factor of 3. For digital preservation, the implications of this slow transfer speed is that, unless a technology breakthrough in data transfer occurs, the feasibility of long-term survival of data in mass storage systems is problematic. At current data transfer rates, migrating a petabyte of data onto new media for preservation could take a decade. Because the life expectancy of the storage media may be only a decade, completing the transfer before a nonrecoverable data loss occurs may not be possible. In other words, data production may out run (and render impractical) data preservation, particularly in mass storage applications.8

This example is not as extreme as it may sound: Some scientific mass storage systems are now acquiring as much as five terabytes of data per day, and many such systems have long-term or permanent retention requirements. Consider the situation at the European Laboratory for Particle Physics in Geneva, Switzerland, which is the world’s largest high-energy particle physics laboratory. This facility operates one of the largest data collection efforts in the world today. The data is of unquestioned scientific value and is
subject to indefinite or permanent retention requirements. The total data generation rate at this facility is nearing 200 terabytes per year, with the potential to reach one petabyte per year. The data is captured onto disk and is subsequently downloaded to magnetic tape cartridges. This lab is now strainning its technical resources to recopy the legacy data on old tape formats onto new, industry standard media. The rate of growth of new data is far faster than transfer rates for the legacy data; however, no viable, long-term solution to this dilemma is in sight.9

**Digital Media Stability**

The term *media stability* refers to the extent to which a given recordkeeping medium retains its physical and chemical properties, or the period of time during which the medium remains useful for its intended purpose. Or, in more practical terms, media stability refers to the ability of various records media to retain their information content in usable form over a given period of time.

Organizations conducting studies on media longevity and its implications for digital preservation included the National Media Laboratory, Boulder, Colorado; the Commission on Preservation and Access (now a part of the Council on Library and Information Resources); the Northeast Document Conservation Center, Andover, Massachusetts; and the Image Permanence Institute at the Rochester Institute of Technology, Rochester, New York.10

The *life expectancy* of records media is defined by the American Society for Testing and Materials as the minimum length of time that information is predicted to be retrievable. For example, LE-1000 would indicate that a record is expected to be usable for 1000 years.11 The actual life expectancy of a particular storage medium for digital data depends on the following factors:

- The quality of the media resulting from its manufacture;
- The quality of the recorder used to write to the media;
- The number of times data resident on the media is accessed during the media life;
- The care with which the media is handled;
- The storage conditions (temperature and humidity);
- The cleanliness of the storage environment.12

With respect to electronic records media, no published stability standards for these media comparable to those for paper and microfilm are available. In the remaining sections of this chapter, we review the stability of various records media, including visible and electronic records media for purposes of comparison. Primary on-line disk storage in mainframe environments and hard disks and other fixed electronic media in network and desktop environments are excluded, because these media are used for processing current records and have no intended utility for long-term data storage purposes. All stability periods mentioned are based on the assumption that premium-grade media stock that has been subjected to proper handling and stored under optimum conditions for the duration of its retention life is used.

**Stability of Media Types**

When deciding which media to use for storage, records specialists usually consider the stability of each media. The following information about commonly used media help them make this decision.

- **Paper.** The stability of paper varies widely by type and quality, depending chiefly on the degree of acidity inherent in its content. The ANSI/NISO standard for Permanence of Paper defines *permanent paper* as the “ability of paper to last at least several hundred years without significant deterioration under normal usage and storage conditions in libraries and archives.”13 At present, several hundred varieties of paper stock manufactured in the U.S. comply with this standard, most at competitive prices when compared to non-permanent papers. Because it is a traditional archival medium having eye-readable information, paper has been universally accepted as appropriate for the permanent preservation of records, even though its stability characteristics may in some cases be less than microfilm. However, poor quality business papers (e.g., thermal fax) are frequently subjected to various archival conservation measures designed to enhance their longevity.

- **Microfilm, silver gelatin type.** Although considered by some to be an old-fashioned solution, silver gelatin microfilm offers perhaps the best permanent keeping properties of any recordkeeping medium; thus, it remains the medium of choice for many archival applications. It is an excellent choice for computer data that does not require long-term preservation in machine-processible format. The newer type of silver gelatin microfilm, of polyester material, provides stability for 500 plus years.

- **Microfiche, diazo and vesicular types.** Diazo and vesicular microfiche provide stability for 100 years.

- **Optical media.** Optical media stability varies from 25 years for WORM to 100 years for CD-R.; CD-ROM is estimated at 25 years.

- **Magnetic diskettes.** Diskettes are the most fragile of the magnetic media; they provide stability for 5 years.

- **Magnetic tapes.** Magnetic tape remains the predominant storage media for the retention of inactive computer data. Its stability varies from 10 to 20 years.

**The Greatest Threat: People, Not Technology**

Commentators almost unanimously agree that technological obsolescence represents a far greater threat to the preservation of digital archives than media longevity. In all
sectors of the hardware and software community, service lives of less than five years are the order of the day. Even the most fragile media will likely exceed the continued availability of readers for these media. Efforts to preserve physical media thus provide only a short-term, partial solution to the general problem of preserving digital archives.

However, technology obsolescence may not be the greatest problem! Organizational commitment, and the willingness to allocate sufficient resources, may be even bigger problems! Digital preservation requires budgets that must be approved by senior executives. These actions must be sustained in the face of reorganizations, mergers, acquisitions, and budget cuts. Any organization contemplating major digital preservation initiatives must confront the question of how sustainable these initiatives will be over time.

**SOME NEW INITIATIVES AND POTENTIAL SOLUTIONS**

We have previously stated that no ideal solution to the digital preservation problem is available today. However, various quarters of the information technology community, as well as the archival profession, are experimenting with a number of developmental solutions, some of which appear to be quite promising. These solutions range from new storage media designed to solve the stability problem, to new archival preservation paradigms designed around preservation practices for digital preservation.

**New Permanent Storage Media**

In 1995, *InformationWeek* ran a brief story under the headline “Digital Media That’s Good for 5000 Years?” that caught the attention of anyone interested in long-term data preservation. The story read as follows:

> Scientists at Los Alamos National Laboratory in New Mexico have developed an information storage technique that can safely archive computer data for up to 5,000 years. Using an ion beam to inscribe data in a space no larger than 560 atoms, the scientists have stored the equivalent of 12,000 diskettes, or 180 CD-ROMs onto an inch-long pin of stainless steel. The high-density, read-only memory devices (HD-ROM) . . . are also capable of archiving images.14

Based on technology invented by scientists from the Los Alamos National Laboratory, Norsam Technologies (www.norsam.com), in Los Alamos, New Mexico, has developed some digital storage products that could potentially revolutionize the world of electronic archives: HD-ROM and HD-Rosetta. The HD-ROM product is designed for the archival storage of digital data, while the HD-Rosetta product is its analog, human-readable counterpart. Engineers at Los Alamos characterized the HD-ROM as a complete departure from existing data storage technologies. They reported that, for the first time, a nonmagnetic, nonoptical data storage system can be made from truly robust materials that are virtually impervious to deterioration over time. The recording materials are very hard, nonmalleable, nonflammable and do not react easily with chemicals. Media stability is estimated to be hundreds if not thousands of years.15

According to John Bishop, Norsam’s President and CEO, “The principal purpose of the HD-Rosetta system is to protect valuable information from destruction and platform independence.”16 Eye-readable data and images can be viewed on any high-powered microscope, thus obviating hardware / software dependencies. The stored images can be transferred from microfilm, paper, CD-ROM, or other media.

To cite just one archival application, the HD-Rosetta system is being used by the Long Now Foundation (www.longnow.org) to create a digital archive of selected languages in use throughout the world. According to the foundation, 50 to 90 percent of the world’s languages are predicted to disappear in the next century, many with little or no significant documentation. The goal of the project is to create a permanent archive of 1,000 languages, resident on the HD-Rosetta media and readable in this analog format by a high-powered microscope.

These new media appear to be very promising as platform-independent solutions for long-term data storage, but whether they will achieve status as a proven archival solution with widespread adoption throughout the U.S. and the world remains to be seen.

**The Emulation Solution**

*Emulation* is the use of a new computer to impersonate an old computer. An *emulator*, then, is a software program that runs on a new computer to make it operate like the old computer. Emulation has been in practical use on computer systems for many years. The aim is to preserve the original software environment in which digital data of long-term value were created. This potential solution to long-term data retention was articulated by Jeff Rothenberg in his seminal essay *Avoiding Technological Quicksand: Finding a Viable Technical Foundation for Digital Preservation*.17

The central idea of this preservation strategy (Rothenberg calls it the only “true solution” yet proposed) is to emulate obsolete computer systems on future, unknown systems, so that a digital document’s original software can be run in the future despite being obsolete. This approach involves developing techniques for the following:

- Specifying emulators that will run on unknown future computers and that capture all attributes required to recreate the content and look and feel of future digital documents;
- Preserving—in human-readable form—the metadata needed to find, access, and recreate digital documents under the emulation methodology; and
- Encapsulating documents and their attendant metadata, software, and emulator specifications in ways that preserve the integrity of these digital objects.

Although this strategy for digital preservation may be promising, it is only in the concept/experimental stage. Among other problems, emulation exposed its users to the increasing possibility that software failures will occur as the old systems continue to age and the pool of expertise concerning them shrinks. Emulation is based on the assumption that the emulated software will continue to run without maintenance. As the year 2000 date-conversion problem showed, this assumption is not a safe one. Further, an emulation approach depends on several components working together—the emulation software, the original application, and the data itself. As the number of components increases, so does the risk of failure.

E-Paper

In June, 1999, Xerox PARC (the company’s research facility located in Palo Alto, California) announced that it will collaborate with 3M Corp. as the manufacturer to bring to market a new product referred to as *Electronic Paper*—a digital document display with the portability of paper. Like paper, the experimental product is thin, lightweight, and flexible. However, like a computer display, it is dynamic and rewritable. A commercial release date for e-paper was not announced; whether the product will achieve commercial viability is not known. Nor, for that matter, are the stability characteristics or the preservation implications.18

Permanent E-Mail

A project conducted jointly by the San Diego Supercomputer Center and the U.S. National Archives and Records Administration shows promise in providing workable solutions to the problem of long-term preservation and access to e-mail messages. Using parallel-processing super computers and extensible markup language (XML), the project team converted one million White House e-mail messages appraised as possessing permanent retention value into a standard, transportable XML format in less than two days.

The InterPARES Project

The InterPARES (International Research on the Preservation of Authentic Records in Electronic Systems) project, which began officially in 1998, was conceived to conduct research into the problem of preserving authentic records over time.19 The initial research focused on the current state of the art in electronic records management and preservation, and to develop and test strategies, both technology and policy-based, for the long-term preservation of electronic records. The principal goals of the project are:

- To identify requirements for preserving electronic records whose authenticity can be verified for an indefinite period of time, regardless of the number of migrations that have occurred from an obsolete technology to a newer one.
- To establish whether the appraisal criteria and methods for determining the retention of electronic records are adequate or whether new ones are required. This process includes methodologies for how electronic records are scheduled for retention.
- To develop new policies, standards, methods, procedures, and rules for preserving electronic records to ensure that they will be useable for as long as they are needed.

Records specialists hope that this and similar initiatives will provide the archival and IT communities with viable solutions to the digital preservation problem.

---

**CASE STUDY:**

**THE ELECTRONIC AND SPECIAL MEDIA RECORDS SERVICES DIVISION, U.S. NATIONAL ARCHIVES**

This case study describes an actual working model of an institution whose sole mission is the preservation of digital data of permanent value.20 The U.S. National Archives and Records Administration (NARA) is the statutorily authorized repository for “those official records which have been determined by the Archivist of the United States to have sufficient historical or other value to warrant their continued preservation by the Federal Government . . .”. The Electronic and Special Media Records Services Division (formerly known as the Center for Electronic Records and hereafter referred to as “the Division”) is the central arm of the U.S. Government for digital preservation. It preserves, and provides public access to federal records in a format designed for computer processing. (See the Division’s home page at www.nara.gov/nara/electronic.)

The data may come from any part of the federal government and may originate in any type of computer application such as word processing, computer modeling, or geographical information systems. Electronic records are accepted into the Division based on traditional archival/records management practices (inventorying, appraisal, and retention scheduling) applied to electronic recordkeeping environments.

The Division has been in business since 1968. It accessioned its first digital records in 1970 from the National Aeronautics and Space Administration (NARA); its oldest digital records date from the 1940s. During its early days, the Electronic and Special Media Records Services Division was known as the Machine-Readable Archives.

---
Division. The Division currently preserves some 152,000 data files—just under three terabytes—from more than 100 federal agencies, bureaus, and departments. The Division currently has 47 staff members, including part-time employees. Databases constitute approximately 95 percent of the holdings. The largest collection is federal census records from the U.S. Bureau of the Census. A catalog of holdings is accessible on the Web (www.nara.gov, Research Room, then Media). Beginning sometime in 2002, the Division plans to make its holdings accessible via the Internet. Using the Internet will permit record-level access to selected databases.

**Appraisal of Archival Data**

Data appraisal is based on a content analysis (an evaluation of the value of the data) and a technical analysis (an evaluation of the usability of the data). The results determine whether, when, and how the records can be transferred from a federal agency's computing environment to the archival environment. NARA's appraisal criteria states that unaggregated micro-level data—data in its original or raw form before aggregation, summarization, or masking—have the greatest potential for long-term research use. Once NARA determines that certain electronic records possess enduring value, it then determines whether the records should be preserved in electronic format, or whether some other format would suffice. For example, computer processing is highly desirable and frequently required for large collections of data that may be subject to statistical analysis; that is, in cases where usage of the data would be significantly impaired, or where the data would be rendered entirely unusable, by preservation in a format other than digital.

**Data Transfer / Accessioning**

Data transfer and accessioning requirements are specified in 36 CFR 1228.270. First, system and software dependencies are analyzed to determine whether they prevent or impair transfer, preservation, or retrieval of the data. Technical documentation adequate to identify, interpret, and service the data must be transferred with the records. Documentation for data files and databases must include record layouts, data element definitions, and code translation tables (code books) for coded data. Documentation is mostly received in paper form.

The data may be transferred onto magnetic tape (open reels or 3480 cartridges). CD-ROM is also accepted as a medium for depositing data in the Division; they must conform to ISO 9660 and ASCII standards. The CD-ROMs may contain other files, such as software and temporary records, but all records appraised for permanent preservation must consist of discrete files that contain only permanent data. Further, digital linear tape has just been authorized as an acceptable transfer medium, and 3590 tape cartridges are under review.21 Finally, data transmission via file transfer protocol (FTP) is acceptable. Scanned image files are not now accepted for preservation, but Division officials expect to begin accepting these types of files in the near future.

The Division will not accession data in formats dependent on specific hardware and software. The records should be written in ASCII or extended binary coded decimal interchange code (EBCDIC) with all control characters and other nondata characters removed. Textual documents should be transferred as plain ASCII files; however, such files may contain standard generalized markup language (SGML) tags. Data files and databases must be transferred as flat files or as rectangular tables.

**Maintenance of Permanent Data**

For all its digital holdings, the Division performs the following maintenance tasks:

- Verification of the data; that is, comparison of the content of the data to the documentation (particularly the record layouts and codes);
- Creation and maintenance of a master and back-up copies (3480 cartridges is the current preservation medium);
- Storage in conformance with environmental standards;
- Annual statistical sampling to identify any loss of data;
- Copying of the data onto new, industry standard media every 10 years.

**Access Restrictions**

Generally, the Division's electronic archives are public records, open to the public. However, the Division adheres to the following restrictions:

- All Freedom of Information Act exemptions based on national security, individual privacy, proprietary interests, or matters protected by specific statute are applied.
- NARA's disclosure restrictions relating to individual privacy generally remain in effect for 75 years. These restrictions apply to federal census data.
- Most statutory restrictions remain in effect until the records are 30 years old. However, in some cases, the Division is authorized to release a disclosure-free version of certain data.
- Under 36 CFR 1256.4, biomedical researchers may be granted access to restricted data for statistical or quantitative research, if they agree in writing to certain conditions and restraints.

**The Future**

As noted previously, during the past thirty years, the Division has preserved and made accessible some three terabytes of digital data. Although these efforts are indeed laudable, this quantity of data is literally a pebble on the beach when compared with the U.S. government's current and future needs for digital preservation. To cite just one
example, in eight years the Clinton White House generated some 40 million e-mail messages in just one of its systems. The National Archives estimates that it may receive something on the order of one billion data files annually by 2009. The problem, of course, is that little or no evidence exists that the National Archives is capable of scaling its digital preservation facilities to accommodate anything like this huge mass of permanently valuable data. To meet the challenge that electronic records pose to its mission, in 1998 the U.S. Archivist established the Electronic Records Archives (ERA) program. This initiative is intended to research, plan, and develop a system that can assemble, manage, preserve, and access electronic records produced by all branches of the U.S. government.22 For more information about this program, visit the ERA program Web site at www.nara.gov/era.

NOTES


3 Svanhildur Boggadottir, E-mail message to David O. Stephens, 9 January 1999.


9 Ibid.


11 Ibid.


16 Ibid.


21 NARA is introducing these transfer methods in order to reduce the media and shipping costs of permanent electronic records accessioned from government agencies, improve record and file integrity, and expand the options for transfer methods. See www.archives.gov/about_us/opportunities_for_comment/transfer_methods_pr.

In the preceding chapter, we introduced the issue of long-term data by reviewing the technical and practical difficulties associated with it. We then discussed some promising new initiatives that will, hopefully, get us closer to what might be considered an ideal solution. We now turn our attention to the how of long-term data retention; that is, technical guidelines and best practices currently employed that are designed to ensure the usability of electronic records for extended periods of time. A sample long-term data retention policy is presented in Figure 11-1.

Perhaps a good way to introduce the current state of the art in long-term data retention is to cite an oft-quoted remark by Dr. John W. C. Van Bogart, principal investigator for media studies at the National Media Laboratory. He states, “Digital archives should be transcribed every 10 to 20 years. To realize lifetimes greater than this, one would be required to:

- Archive the recording system and media,
- Archive the system hardware and software,
- Archive the operating system,
- Archive operations manuals,
- Archive ample spare parts.”

This somewhat wry statement suggests that the museum approach, in which these components of a particular computing environment must be preserved in a museum-like environment (along with the data itself) in order to accomplish future processing, is required. Although such an environment is not literally the case, the statement does provide a good point of departure for our discussion concerning the how of digital preservation.

ISO 15489: DATA PRESERVATION PRACTICES

In the technical report that accompanies ISO 15489, the new international standard for records management, the issue of digital preservation is addressed. Section 4.3.9.2 addresses the issue of continuing retention. The report states:

Preservation strategies for records, especially electronic records, may be selected on the basis of their ability to maintain the accessibility, integrity, and authenticity of the record over time, as well as for their cost-effectiveness. Preservation strategies can include copying, conversion, and migration of records. . . . Other methods may be used to retain electronic records for long periods, as new technologies become available. Strategies for retaining electronic records and associated metadata removed from systems have to be formulated and integrated into all system design processes to ensure that the records and associated metadata will remain accessible and usable for the entire period of their retention.

Each of the preservation practices mentioned in this standard is addressed in the remainder of this chapter.

BEST PRACTICE NO. 1: SELECT DATA FOR PRESERVATION BASED ON SOUND APPRAISAL METHODOLOGY

In the world of physical records, archival appraisal decisions tended to be based on qualitative judgments. For example, “These are interesting records; it would be a shame if they were destroyed; some researcher might use them sometime—let’s go ahead and preserve them.” In these environments, however, preservation costs were not too burdensome; relatively modest expenses for shelf space and finding aid preparation expenses.

With electronic records, on the other hand, the expense and technical complexity associated with the permanent preservation of digital archives are such that the benefits of preservation should be demonstrable. At a minimum, these benefits should demonstrate a high degree of expected usage. Therefore, we recommend that the following criteria be applied when appraising electronic records to establish their archival value for permanent retention, or their archival permanence. Digital data should be preserved permanently in computer-processible format:

1. When the value of the data and the benefits of preservation have been clearly established. The value of the data should be substantial and the benefits of preservation should be demonstrable if not compelling.
2. When preservation of the data in manipulatable, computer-processible form is required to support significant research objectives.
3. When conversion of the data from a dynamic to a static state—from digital to microfilm format—would severely diminish its value or render it unus-
LONG-TERM DATA RETENTION

SCOPE / COVERAGE: Enterprise-wide, including all business units that must retain computer data for time periods ranging from a minimum of five years to ten years or longer.

POLICY STATEMENT: All departments and business units will implement a formal program, based on the practice guidelines contained herein, designed to assure the long-term retention of computer data in useable form where such is required by the Records Retention Schedules.

BACKGROUND / PURPOSE: To date, ABC’s practices concerning the long-term preservation of digital data have been limited mainly to performing periodic data migrations; that is, converting older computer data requiring continuing retention to new hardware and software environments during the course of implementing system upgrades. The company does not now have a formal digital preservation program to include tape maintenance plans, requirements for the preservation of systems documentation, media recopying or refreshing, or requirements to standardize data formats or media types based on their preservation characteristics.

Formal practices for long-term data retention become important in cases where computer data must be retained in excess of five to ten years—time periods that typically exceed the service lives of hardware and software on which computer data must be processed, or time periods exceeding the ability of certain computer storage media to retain the records residing on them in usable form.

As ABC transitions from a paper-based to an all-digital recordkeeping environment, this policy and its accompanying practices will become more important, even critical, to ensure that computer data that must be retained for long periods of time retains its integrity and usability. Many of the company’s product development records and many other business-critical applications (most of which exist in digital form) must be retained for extended periods of time. These digital preservation requirements are certain to grow in the future.

PRESERVATION REQUIREMENTS:

- For all data required to be retained for retention periods from five to nine years, the practices appearing herein must be evaluated to determine whether they should be implemented.
- For all data required to be retained for ten years or longer, these practices must be implemented.

RESPONSIBILITIES:

Records Management Department

The Records Management Department is responsible for the following:

- Developing formal practices for digital preservation / long-term data retention sufficient to ensure the preservation in useable form of all company computer data that must be retained for extended periods of time.
- Ensuring that all computer data requiring long-term retention is properly scheduled for the appropriate retention periods in the Records Retention Schedules.
- Working with the Information Technology Department to implement the long-term data retention practices specified herein.
able in order to satisfy required (rather than “nice to have”) research objectives.

4. Finally, appraisal decisions to preserve electronic records permanently should be supported by cost-benefit analysis whenever appropriate. In many instances, qualitative appraisal judgments unsupported by such analysis will not be sufficient to make a solid business case for permanent preservation of the data.

Reappraisal to Nondigital / Nonpermanent Status

In physical recordkeeping environments, archival institutions rarely reappraised records once they had been accessioned. The presumption is that once accessioned, the institution was obliged to retain them permanently. In electronic recordkeeping environments, however, this archival principle should be revised. Even though they have been scheduled for permanent retention and, in fact, accessioned into the archives, the institution may, at some point, conclude that it is justified to downgrade the status of certain electronic records from digital format to, say, microfiche format, if the degree of usage does not warrant continued preservation in computer-processible format. Or, lack of usage may justify reappraisal and disposal of the records entirely.

BEST PRACTICE NO. 2: SELECT APPROPRIATE STORAGE MEDIA

A systematic approach to the storage of data subject to long-term or permanent retention requirements must begin with the selection of appropriate blank (unrecorded) media. Media selection should be based on the ability of the media to provide the greatest stability and resistance to obsolescence. The following guidelines are recommended:

- **Adhere to relevant standards.** Data recording and storage media to be used for important information should conform to specifications contained in national and international standards. Such standards have been developed for most types of magnetic tapes, 3.5-inch diskettes, and certain optical media, including magneto-optical (MO) disks and compact disks (CDs). Data storage should be limited to high-quality magnetic or optical media from proven manufacturers. Compared with less expensive, generic products, brand-name magnetic media are manufactured from higher-quality materials and subjected to more rigorous manufacturing and testing processes. Computer media must comply fully with specifications established by the manufacturer of the equipment on which the media will be recorded or played.
  - **Purchase only new media.** Computer media intended for long-term retention of important information should be purchased new. Recycled media; that is, magnetic tapes, diskettes, or rewritable optical disks previously used for data recording should not be used for storage copies of data scheduled for long-term retention.
  - **Purchase premium grade media stock.** Some vendors offer several grades of computer media with varying performance and price characteristics. Although standard-grade media are acceptable for routine information processing, media of the highest available quality are recommended for storage copies of data scheduled for long-term retention. Such super premium media are more likely to produce error-free recordings and preserve high signal levels in storage.

NARA Media Guidelines

The following computer storage media have been selected by the U.S. National Archives as appropriate for the preservation of electronic records required to be retained permanently.

- **Magnetic tape** – Use open reels or tape cartridges. Open-reel magnetic tape must be on 1.5-inch nine-track tape reels recorded at 1600 or 6250 bits per inch (bpi) that conforms to ANSI X3.39-1986, American National Standard: Recorded Magnetic Tape for Information Interchange.

The National Archives also emphasizes the importance of selecting media for long-term archival storage based on the portability of the media; that is, media that will run on equipment offered by multiple manufacturers must be selected, while preserving the ability to transfer the records from one medium to another (i.e., from optical disk to tape).

BEST PRACTICE NO. 3: PERFORM DATA MIGRATIONS

Data migration—a routine practice performed by all IT departments—involves a set of organized tasks designed to periodically transfer digital material from one hardware /
software configuration to another, or from one generation of technology to a subsequent generation. In the context of long-term data retention, the purpose of data migration is to preserve the integrity of the records and to retain the ability to retrieve, display, and otherwise use them over time. Data migration may occur when hardware and/or software become obsolete, or the practice may be employed to transfer electronic records from one file format to another.

During the migration process, the original sequence of the structural and data elements of digital records is rearranged to conform to the newer configuration. The major risk with this digital preservation practice is the risk of altering records during conversion from the source to the target format. For migrations to be executed successfully, those performing them must have knowledge of the original application and data formats. Also, with a more complex file structure, this knowledge is more important. With each successive format conversion over time, the possibility of data loss or corruption increases. Thus, migration is at best an imperfect solution as it can lead to the loss of record integrity.

When performing these data migrations, IT departments should adhere to the requirements of a records retention schedule in making decisions as to whether some, none, or all the older legacy data needs to be migrated to the new environment.

**BEST PRACTICE NO. 4: STANDARDIZE FILE FORMATS**

This data preservation strategy refers to the adoption of one or more standard formats for recording electronic records onto digital media. The particular type of coding scheme employed in creating text, data, or image files can have important implications concerning the ease with which digital records can be read and processed over time on a variety of computing devices. In a preservation context, the most important consideration is that a generic document format be universally useable, standard in technical specifications over time, and sufficiently robust in capabilities to allow accurate, authentic content preservation and document format presentation.

To be universally usable, a document format must be readable without regard to the specific software available on individuals’ desktops. For image and textual data, TIFF Group 4, portable document format (PDF), standard generalized markup language (SGML), and ASCII are the most common file formats in use for long-term retention of image and textual data. Open, nonproprietary file specifications theoretically give TIFF, SGML, HTML, and XML a technical edge for long-term document preservation. However, none of these **markup languages** are in common use on the desktop computer systems of most document creators.

**Extensible Markup Language (XML)**

Archival institutions throughout the world are now considering the potential use of extensible markup language (XML) in digital preservation initiatives, and some are beginning to mandate its use. XML is a flexible, nonproprietary set of standards for annotating or tagging data with semantically rich labels—human readable—that permit computers to process files on the basis of their meaning. XML is called *extensible* because it is not a fixed format; rather, it is actually a *metalanguage*, a language for describing other languages. Several attributes of XML make it attractive for digital preservation applications. The semantic nature of XML tags makes XML suitable for recording metadata. Its extensibility allows archival institutions to expand their systems to accommodate evolving needs. As an open standard, XML reduces if not eliminates the problem of proprietary software. Further, because they are basically text files, XML files can be readily interpreted by disparate computer systems. Finally, the human-readability of XML tags permits archival records to be preserved on paper as well as computer media so that they will be automatically readable through optical character recognition.

**The ASCII Format**

For text files, the ASCII format provides the broadest compatibility for file interchange across platforms and has thus enjoyed wide acceptance in support of long-term data preservation requirements. Organizations should not record data having lengthy retention requirements on proprietary formats; that is, on formats dependent on specific hardware and software.

**The Portable Document Format (PDF)**

The portable document format (PDF), a product of Adobe Systems, has become a de facto standard for providing universal access to electronic documents over the Internet. This file format preserves all the fonts, formatting, graphics, and color of any source document, regardless of the application used to create it. The American National Standards Institute (ANSI) has granted a provisional standard status to Adobe for their PDF format. PDF files can be created from most any desktop application with the full version of Adobe Acrobat software. A PDF capability to link document metadata in XML formats to PDF files is under development.

The Global Electronic Records Association and Collaborative Electronic Systems Association are currently working with Adobe to assist them in moving PDF into a true life cycle preservation format. Although PDF will be the file format of choice in certain preservation situations, issues associated with metadata capture and other technical issues will render it inappropriate in others. Digital preservation planners should remember that the best solution for long-term retention of electronic documents will vary with the business application and the expectations of document usage over time.

**NARA File Format Guidelines**

In order to provide the greatest flexibility for future processing of archival data, the U.S. National Archives has
promulgated the following technical guidelines for federal agencies:

- Utilize either ASCII or EBCDIC formats, with all control characters and other nndata characters removed. The data compression should not be used.
- Electronic textual documents should be preserved as plain ASCII files; however, such files may contain standard generalized markup language (SGML) tags.
- Databases and data files should be preserved as flat files or as rectangular tables (i.e., as two-dimensional arrays, lists, or tables). Each data element within a record should contain only one data value.
- A record should not contain nested repeating groups of data items. The files should not contain extraneous control characters, except record length indicators for variable length records, or marks delimiting a data element, field, record, or file.
- If records or data elements in different files need to be linked or combined, then each record must contain one or more data elements that constitute primary and/or foreign keys enabling various linkages between the related records in separate files.\(^7\)

**BEST PRACTICE NO. 5: ADDRESS METADATA ISSUES**

In the context of long-term data retention, metadata is essential for managing record objects throughout their entire life cycle. The long-term preservation of electronic records in hardware / software independent formats requires that such records be linked to information about their structure, context, and use history. Such metadata must include information about:

- The source of the records;
- How, why, and when the records were created, updated, or changed;
- The intended purpose or function of the records;
- How to open and read the records;
- The terms of access of the records;
- How the records are related to other software and data used by the creating organization.

These metadata must be sufficient to support any changes made to records through various generations of hardware and software, to support the reconstruction of the decision-making process, to provide audit trails throughout a record’s life cycle, and to capture internal documentation. Without an adequately defined metadata structure, digital preservation initiatives cannot be supported.

The most well-known metadata initiative, the Dublin Core Metadata Element Set, has the specific aim of enhancing information accessibility in computing environments, but much attention has recently been devoted to its potential utility in digital preservation initiatives. In fact, in the opinion of some commentators, metadata is *the* best way to manage electronic records over time. Even when digital information has been migrated to new formats, the need remains for users to be sure the document or information object they are looking at is the one they were looking for. Metadata thus plays a key role in facilitating the intellectual as well as physical preservation of these objects over time.\(^8\)

Proper management of metadata is essential to preserve the integrity of record objects for as long as they must remain in a computer-processible format. The metadata must support the authenticity and reliability of the record objects—their structure and context as well as their content—for the full duration of their retention life. The following definitions apply:

- **Content** includes the words, numbers, sounds, and images made by the record’s creator.
- **Structure** refers to the appearance and arrangement of the record’s content. It includes the meaning of a record as conveyed by the appearance of its characteristics (i.e., typeface), the location of specific data fields on the document (i.e., a form), and the pointers used to link physical or logical groups of data.
- **Context** includes the background information describing the origin of the record; that is, which organizational unit created the record, who used it, the purpose for which it was used, and how it relates to other records.
- **Reliability** refers to the ability of a record to stand for the facts it contains; that is, the trustworthiness of the record’s content. It must be trustworthy based on its mode (method by which it is communicated over time and space), form (format or media on which it is created or received), state of transmission, and the manner of its preservation.
- **Authenticity** refers to the fact that a record is what it purports to be and has not been tampered with or otherwise corrupted since its creation; that is, it is proven reliable over time. The record must be genuine and determined to have been managed by specific records custodians through all phases of its life cycle. Authentication of a record is critical in the context of digital preservation because electronic records can only be preserved by copying or reproducing them.\(^9\)

These attributes must be captured at the time of creation of electronic records, and any preservation initiatives must include consideration of how they will be addressed.

**BEST PRACTICE NO. 6: PRESERVE SYSTEMS DOCUMENTATION**

This practice is a key component of long-term data retention because, without the requisite documentation, applications containing such data cannot be processed. The long-term preservation of digital data requires maintaining up-to-date documentation about all systems applica-
tions adequate to understand the purpose and functions of the system, define the contents of the files and records, and specify all technical characteristics necessary for reading and processing the records.

Adequate technical documentation necessary to read and process electronic records over time would include the following:

- A narrative description of the system and data showing the physical and technical characteristics of the records, including:
- A record layout that describes each field including its name, size, starting or relative position;
- A description of the form of the data (i.e., alphabetic, zoned decimal, packed decimal, or numeric); or
- A data dictionary or the equivalent information associated with a database management system, including a description of the relationship between data elements in the database;
- Any other technical information needed to read and process the records.

Documentation for data files and databases would generally include record layouts, data element definitions, and code translation tables (codebooks) for coded data. Data element definitions, codes used to represent data values, and interpretations of these codes must match the actual format and codes.10

**BEST PRACTICE NO. 7: STORE MEDIA PROPERLY**

If they are not stored under good environmental conditions, the life expectancy of storage media, and the electronic records residing on them, can be expected to suffer. The basic rule-of-thumb is cool, dry, and free of fluctuations. The two organizations that have issued the most authoritative pronouncements relating to media storage for purposes of long-term data retention are the U.S. National Archives, which prescribes storage standards applicable to the federal government, and the American National Standards Institute (ANSI), which has issued a standard pertaining to the storage of imaging and magnetic media. The technical guidelines of both these organizations are reviewed next.

**ANSI Standard for Media Storage**


1. **Medium-term storage conditions.** Conditions suitable for the preservation of recorded information for a minimum of 10 years.
2. **Extended-term storage conditions.** Conditions suitable for the preservation of recorded information of permanent value.

**Temperature and Humidity Conditions**

The ANSI standard states that protection against environmental damage is enhanced when magnetic tapes are stored at a low temperature and relative humidity, but very low temperatures can lead to separation of tape lubricants from binder materials. The following guidelines are recommended for medium- and extended-term storage:

- **Medium-term storage.** The ANSI standard specifies a maximum temperature of 25 degrees Celsius (77 degrees Fahrenheit) for extended time periods and 32 degrees Celsius (90 degrees Fahrenheit) for short periods of time. The recommended relative humidity is 20 to 50 percent. Temperature variations in the storage area must not exceed 2 degrees Celsius (4 degrees Fahrenheit) over a 24-hour period. Humidity variations must not exceed 10 percent over a 24-hour period. The minimum acceptable storage temperature is 8 degrees Celsius (46 degrees Fahrenheit).

- **Extended-term storage.** The ANSI standard specifies three combinations of temperature and relative humidity:
  1. A maximum temperature of 20 degrees Celsius (70 degrees Fahrenheit), with relative humidity ranging from 20 to 30 percent;
  2. A maximum temperature of 15 degrees Celsius (60 degrees Fahrenheit), with relative humidity ranging from 20 to 40 percent; or
  3. A maximum temperature of 10 degrees Celsius (50 degrees Fahrenheit), with relative humidity ranging from 20 to 50 percent.

- **Fluctuations.** As the storage temperature rises, relative humidity must be more tightly controlled. Temperature variations in the storage area must not exceed 2 degrees Celsius (4 degrees Fahrenheit) over a 24-hour period. Humidity variations for extended-term storage must not exceed 5 percent over a 24-hour period.

**NARA Requirements**

Organizations should maintain the storage and test areas for computer magnetic tapes containing permanent records at the following temperatures and relative humidity:

- Constant temperature of 62 to 68 degrees Fahrenheit;
- Constant relative humidity of 35 to 45 percent.12

**Storage of Blank Media Stock**

Prior to use, computer media should be stored under conditions specified by the manufacturer. In most cases, the temperature in the storage area should range from 5 to 48 degrees Celsius (41 to 120 degrees Fahrenheit), with a relative humidity of 20 to 80 percent.
Air-conditioned Storage Facility

For both medium- and extended-term storage, the ANSI/NAPM IT9.23 standard specifies an air-conditioned facility to maintain the temperature and humidity limits delineated previously. Specialized air-conditioning equipment may be necessary to maintain low temperatures within the specified humidity ranges. A clean, dust-free storage environment is essential.

Air-conditioning is usually necessary for removal of pollutants as well as temperature and humidity control. Although most air-conditioner filters will capture dust particles measuring 10 microns or larger, much smaller particles can damage high-density magnetic tape recordings. Electronic air filters are typically required to trap such particles. The ANSI/NAPM IT9.23 standard cautions against gaseous impurities such as ammonia, chlorine, peroxides, smoke, sulfides, and oxides of nitrogen. Where air-conditioning is not practical or required, as in underground storage areas with low temperatures, dehumidification will typically be necessary.

Cleanliness of Storage Facility

The ANSI standard prescribes that media storage areas must be cleaned regularly. To minimize scattering of dust particles and other potentially harmful contaminants, proper housekeeping habits must be observed. For magnetic tape libraries, the ANSI standard specifies a vacuum system with an exhaust pipe that evacuates dust from the storage area. Static-free, chemically inert wipes are recommended for cleaning shelves and media containers. Ordinary dust rags, steel wool, abrasive cleaning materials, or chemical cleaning solutions should not be used. Floors should be dry-mopped or cleaned with a minimum amount of water followed by dry-mopping. Floor wax and buffing machines can generate debris from abrasions caused by foot traffic.

Media Shelving / Housing

The ANSI standard specifies that computer media should be shelved in the upright, vertical position to prevent warping of containers. Media should never be stacked horizontally; storage containers should not support the weight of other containers. Magnetic tape reels should be enclosed in wrap-arounds when not in use. Computer tape cartridges, optical disks, and other media should be stored in protective containers when not in use. To prevent the accumulation of dust and other contaminants, containers should be closed at all times, even when they are empty.

Safety and Security

The ANSI standard addresses the issue of magnets and any other objects that generate magnetic fields, and notes that such items are forbidden in media storage areas. To prevent accidental overwriting of information intended for long-term storage, write-enable rings should be removed from magnetic tape reels. With diskettes, magnetic tape cartridges and cassettes, and optical disks, write-protect tabs or other recording inhibitors should be activated.

By definition, storage copies of computer media should be utilized as little as possible, because any reference activity subjects them to possible damage from improperly adjusted equipment or careless handling. If frequent reference to a given computer medium is anticipated, one or more working copies should be made.

Combustible materials are forbidden in storage areas. Carbon dioxide or other dry fire-protection methods should be employed. The method selected must not produce potentially harmful residues.

Computer media that contain vital information should be duplicated for storage at a secondary site. Storage precautions and environmental controls outlined previously should be implemented.

BEST PRACTICE NO. 8: PERFORM PROPER MEDIA MAINTENANCE TASKS

In situations where organizations store long-term data on magnetic tapes, certain maintenance practices are required to ensure that the data retains its integrity, in usable form. Both ANSI and the U.S. National Archives have issued technical guidelines addressing these matters. These guidelines are reviewed next.

Media Recopying

Media recopying has long been a key data preservation practice. The practice involves recopying the data residing on old media onto new, industry standard media at regular intervals, sometime prior to the expiration of the media life expectancy. If new media are used, periodic recopying can extend the life of recorded information indefinitely, thereby effectively overcoming problems associated with the nonarchival nature of computer media. Copying can also be used to transfer information from deteriorating or obsolete media onto new media. Digitally coded information can be copied an indefinite number of times without degradation. To minimize the adverse effects of temperature and humidity variations, media copying should be performed in the long-term storage environment.

NARA requires that organizations copy permanent data onto industry standard tested and verified new magnetic tapes before the tapes are ten years old. The ANSI standard states that in order to provide additional protection against permanent error conditions that can render information irretrievable, the contents of computer media should be copied onto new media at regular intervals. No time period is specified, however.

To minimize risks associated with defective media, organizations should create two or more storage copies of very important information intended for long-term retention.
Media Inspection

To facilitate early detection of tape stress, evaporation of lubricants, or other dangers to recorded information, computer media in long-term storage should be inspected regularly. The ANSI standard recommends inspection of magnetic tapes at five-year intervals, with more frequent inspections if temperature and humidity deviations have occurred. Inspection intervals for other computer media are not defined by national or international standards. Inspection should involve a visual examination of media and their housings, followed by the retrieval or playback of recorded information. In a large collection of computer media, a portion of the collection can be sampled. If permanent errors are detected in the sampled media, the entire collection must be examined.

NARA’s technical guidelines specify that organizations should read a statistical sample of all reels of magnetic tapes containing permanent records to identify any loss of data and to discover and correct the causes of data loss. In tape libraries with 1,800 or fewer reels, a 20 percent sample or a sample size of 50 reels, whichever is larger, should be read. In tape libraries with more than 1,800 reels, a sample of 384 reels should be read. Tapes with 10 or more errors should be replaced with new industry standard media and, when possible, lost data should be restored. All other tapes that might have been affected by the same cause (i.e., poor quality tape, high usage, poor environment, improper handling) should be read and corrected as appropriate.

NARA’s guidelines also provide that organizations should test magnetic computer tapes no more than six months prior to using them to store electronic records scheduled for permanent retention. These tests should verify that the tapes are free of permanent errors and are in compliance with applicable standards promulgated by the National Institute of Standards and Technology (NIST) or other relevant industry standards.

Media Refreshing / Rewinding

Rewinding is a procedure intended to maximize the life expectancy of data resident on magnetic tapes by unspooling and rewinding the tapes to relieve stresses. Refreshing involves transcribing and rewriting the data in order to refresh the magnetic signals and prevent or minimize data loss. To minimize the likelihood of cinching, magnetic tapes can undergo a slow wind / rewind cycle to obtain a smooth, evenly tensioned pack prior to storage or prior to initial use after removal from storage.

In the past, various authorities have recommended that magnetic tapes in storage be rewound at regular intervals, perhaps annually, to alleviate accumulated stress or to tighten loose tapes. Such rewinding is described as exercising or retensioning a tape. At present, however, wide disagreement exists among the several parties having an interest in this matter as to its necessity or desirability, and a definitive recommendation for or against periodic rewinding cannot be provided. Recent research suggests that periodic rewinding of magnetic tapes may not be necessary, particularly for magnetic tape cartridges or cassettes with small diameters.

The U.S. National Archives specifies in its technical guidelines that organizations should rewind under controlled tension all tapes containing permanent records every 3.5 years. However, the National Archives is reportedly discontinuing periodic rewinding of its magnetic tapes, presumably because they do not consider this procedure required to assure the integrity of their archival data.

The ANSI standard is notably silent on this issue; periodic rewinding is not mentioned in its discussion of tape tensioning. Based on its own test results, Imation, the leading manufacturer of magnetic storage media, recommends against periodic rewinding of quarter-inch magnetic tape cartridges, although it does recommend a full unwinding and rewinding to exercise stored tapes immediately prior to use. Ampex, by contrast, recommends that metal particle tapes in storage be retensioned at five-year intervals to relieve stresses.

Media Acclimatization

Computer media removed from an environmentally controlled storage facility and taken to a work area with different environmental characteristics should be acclimated to the new environment before use to prevent moisture condensation. According to the ANSI standard, temperature acclimatization for magnetic tapes can take 30 minutes to 4 hours, depending on the type of medium. Humidity acclimatization is a slower process, requiring one day to several weeks or longer. Wider tapes require longer acclimatization times than their thinner counterparts.

The acclimatization process can be accelerated by unwinding and rewinding a magnetic tape several times, thereby exposing more of the tape surface to the new environment. Exposed media will achieve thermal equilibrium in seconds and moisture equilibrium in minutes. Computer media intended for long-term storage should be returned to an environmentally controlled facility immediately after use.

NOTES

3 For a good general summary of selecting data storage media to support long-term preservation requirements, see Charles M. Dollar, “Selecting Storage Media for Long-Term Access to Digital
4 These and other data preservation requirements were extracted from printed leaflets of The Electronic and Special Media Records Services Division, U.S. National Archives and Records Administration (NARA). See also the Division’s home page at www.nara.gov/nara/electronic.


7 Ibid., NARA Guidelines.

8 See, for example, Michael Day, “Extending Metadata for Digital Preservation.” Available at www.ariadne.ac.uk/issue9/metadata/.


10 Ibid., NARA Guidelines.

11 American National Standards Institute, ANSI/NAPM IT9.23-1996, *American National Standard for Imaging Materials—Polyester Base Magnetic Tape—Storage*, (Washington, DC: ANSI, 1996). We are particularly indebted to Dr. William Saffady for his analysis of and interpretative judgments concerning the use of this standard, which are reflected throughout this narrative.

12 Ibid., NARA Guidelines.
Most of the preceding chapters have been devoted to the principles of developing records retention schedules that provide customized coverage for an organization’s computer data. These schedules are, however, merely a policy statement—words printed in three-ring binders or, more recently, on intranet Web sites. They are of no value to any organization unless they are properly implemented. This chapter discusses how to accomplish this most important element of any enterprise electronic records retention initiative, without which the concept of managing the life cycle of computer data can ever become a reality. Because we covered implementation for archival data of permanent value in the preceding chapter, our main focus here is on the implementation of retention policies for data of temporary value.

In order to implement retention policies for such data, three key steps are required:

1. Development and implementation of a new policy requiring the IT department to implement data retention functionality in all software applications requiring it.
2. Annual or periodic records purge days to dispose of all data eligible for this action in accordance with the records retention schedules.
3. Periodic audits to determine the status of compliance with the enterprise records retention program.

**COMPREHENSIVE DATA RETENTION FUNCTIONALITY**

In order to implement electronic records retention policies, the software used to process and manage data must have the capability to recognize expired data and purge it from the system, as required by the records retention schedules. Various system utilities are required to accomplish these steps, as follows:

- **Data flags.** As defined in Chapter 5, a data flag is a software utility for identifying the point in time when electronic records make their life cycle transition from an active to a semiactive or inactive state. This record status change may indicate that the data is eligible for migration from primary to secondary storage media.

- **Data purge routines.** As also discussed in Chapter 5, data purging is defined as the automatic erasure of useless electronic records, effectuated by means of purge functionality, based on predefined electronic retention periods that have been incorporated into the design criteria of a computer application. Purge functionality is any set of programmed instructions built into applications programs or installed as a system-wide utility to identify expired data and effectuate its disposal. These actions should occur under the authority of an electronic records retention schedule.

**Other Data Retention Capabilities**

Although data flagging and purging are indeed key components of any electronic records retention initiatives, the software needs to be capable of more than identifying expired data and removing it from the environment. In order for the electronic records retention program to be complete, more robust data retention functionality needs to be incorporated into the software for all applications containing data scheduled for disposal.

As provided by the sample application software retention policy presented in Figure 12-1, each software application must provide a method for defining and implementing retention requirements for all records created and maintained by that application. Each software application must provide a method for identifying electronic records eligible for destruction when their retention periods have elapsed. Moreover, each software application must provide a method for determining destruction dates for specific electronic records based on retention periods in the records retention schedules. Consequently, the software must be able to mark electronic records for deletion and provide a list of such records for approval by business owners or other parties prior to deletion.

Further, each software application must be able to actually effectuate the destruction of expired data; it must permit the safe and complete deletion of electronic records approved for destruction. As used here, the term complete deletion means irretrievable and nonrestorable; that is, the software application must prohibit the recovery of deleted records through backups, mirror image directories, undelete commands, or other mechanisms. Finally, each software application must maintain a log or other information about electronic records that have been deleted.
Data Retention Functionality is Frequently Ignored. Why?

For the large majority of computer applications, purge routines and other functionalities have not been built into the original systems design, or if they were, they have not been based on a well-conceived retention schedule fully developed and implemented at the application level. Possible reasons for this oversight might be one of the following:

- The need for data purging may not have occurred to users when they enumerated needs to be considered in designing systems.
- A lack of standards or policies dictating that purge routines must be designed into all system applications.
- Requirements for purge routines exist, but they are not implemented or enforced.
- Under pressure to complete and deliver a system application, the purge feature was relegated to a subsequent maintenance phase, which was never completed.
- As storage costs declined, the idea of free storage permeated the thinking of a generation of systems developers to a point where purge routines and the scarcity of space were considered to be unnecessary, and they were not built into systems.

Software Retention Functionality Scenarios

New and existing software applications vary widely with respect to functionality needed to comply with records retention requirements. The most frequently occurring scenarios are described next, with suggestions for complying with these requirements:

- **Scenario 1.** The software has the required data retention functionality, and it is being properly implemented. This scenario is, of course, the best-case scenario; the goal is to assure that no new problems arise during the execution of the purge routines.
- **Scenario 2.** The software has the required data retention functionality, but it is not being implemented. In these situations, records and IT specialists should develop a plan to implement this functionality during records purge days.
- **Scenario 3.** The software has some data retention functionality, but further development is required. Records and IT specialists should devise a plan to develop means of implementing the required functionality according to IT practices for software development. Implementation can be scheduled as a separate task, or it can occur at the time of the next software upgrade.
- **Scenario 4.** The software has no data retention functionality, but it can be incorporated. In these situations, records and IT specialists should develop a plan to assure that standard life cycle functionality is incorporated. Life cycle functionality should normally occur at the time of the next system upgrade.
- **Scenario 5.** The software is supplied by third-party developers, who refuse to incorporate the required data retention functionality. Assuming that such functionality is required in order to execute the retention policy, organizations should not purchase or implement this type of software if at all possible. In cases where such software has been previously purchased, the organization should exert any and all pressure on the software vendor to incorporate this functionality at the earliest possible time.

When to Incorporate Purge / Retention Functionality

In the absence of purge routines and the flagging of inactive records, existing systems must be changed first to identify, then to extract / remove inactive records from data files. These change requests will often receive a very low priority, given the typical amount of backlog for new development and systems maintenance. The following strategies can assist IT specialists in accomplishing the change requests:

- Seek management support for moving records retention to a priority project for cost savings or mitigating liability if the amount of data is either especially large or particularly sensitive.
- Employ query tools to run ad hoc sweeps of data files to identify inactive records based on a predefined criteria identified on the approved retention schedule. The same ad hoc tools can be employed to remove useless records.
- Wait until a particular application is scheduled for conversion to another system or is scheduled for major systems maintenance.

Data processing standards should be established to require purge routines in the initial stage of application development. Although the design and analysis needed for comprehensive data retention functionality can be fairly complex, building in these utilities upfront is preferable to adding them later. Retrofitting existing systems with retention functionality after they are up and running is much more costly and difficult than in original development.

The following example illustrates the situation. It is a summary of the status of data retention functionality in software applications at ABC Corporation, the fictitious name for a large multinational manufacturing firm.

- Total number of system applications – 816
- Total number of application programs supporting those system applications – 34,000
- Estimated number of programs with purge logic – 3,400 or 10%
- Number of application programs requiring review in order to ascertain retention status and possible coding for purge logic retrofit – 6,120 or 20%
- Analysis and programming time to retrofit each program – 2 days
- Total days to complete purge logic retrofit – 12,240 or 55 person-years
A NEW INFORMATION TECHNOLOGY (IT) POLICY FOR ELECTRONIC RECORDS RETENTION

What conclusions can be drawn from this example? The inference is clear: No IT department has or can allocate 55 person-years of programming time, or any other large commitment of resources, to retrofit data retention functionality into all applications that require it. For all but the smallest organizations, enterprise implementation of electronic records retention will require a multiyear commitment on the part of IT. Further, to attempt to retrofit functionality into existing applications is usually not a feasible strategy. For most organizations, the only feasible strategy for incorporating purge functionality into all applications software requiring it is to adopt a new IT policy requiring that such functionality be incorporated at the time of the next technology upgrade. A sample policy—Software Applications: Records Retention Requirements—is provided in Figure 12-1.

Data Retention or Purge Days

The use of records purge days as a prime strategy for implementing the electronic records retention program is strongly recommended. The reason is that they work; they are the single most effective step in retention implementation. In fact, unless the organization is prepared to utilize this method of implementation, it should probably not bother with trying to do records retention at all! In implementing enterprise electronic records retention initiatives, two separate sets of data purge days are required:

- **IT Purge Days.** These days are designed to effect the disposal of all data residing in system applications managed by the IT department. These purge days for shared data are often difficult to conduct when time schedules under which data centers operate are tight. Extra time (an extra hour or two) is almost unheard of in data centers operating around the clock, seven days a week. When purge routines are built into applications systems, they are considered a part of regular processing and time is allotted for them. Ad hoc identification and purge, particularly on voluminous files, might take several hours to run. Time for purging large files may have to be specially scheduled, long in advance.

- **Desktop Purge Days.** As discussed in Chapters 6 and 7, these days are designed to effect the deletion of all user-controlled PC-based records kept at the desktop level. Records purge days can be an excellent means of applying the electronic records retention schedules to dispose of user-controlled electronic records in PC-computing environments. All PC users would be required to review directory listings and delete all documents and data (including e-mail) eligible for such action from their hard drives, from any central network server, and from removable media (diskettes). Whether these PC records possess the status of official records, or whether they merely serve as a means of production of official hard copy documents will often be the basis of decisions on whether to purge these files.

We recommend that requirements for these data purge days be incorporated into any policies and procedures relating to electronic records retention and its implementation.

Data Retention Audits

As with any effective, visible media schedule, an electronic records retention schedule requires a periodic audit to assure compliance with company policy. The obvious place for such auditing is within an existing internal audit structure whose mission is to perform periodic departmental audits to determine the degree of adherence to established company, industry, and/or legal standards. Many internal audit departments have a specific unit devoted to auditing electronic-based data; others have routinely incorporated this function into the general audit procedures. Records specialists may need to either initiate or participate in compliance audits, particularly soon after the implementation of the records retention schedule or if any evidence exists that the audit is not being done on a regular basis. Part of the audit process should be to confirm that the complete destruction of all data scheduled for disposal has actually occurred; merely placing a magnetic tape into a scratch bin is not sufficient to comply with a destruction order.

If an internal audit function is not being conducted, records specialists are responsible for reminding business owners, users, and IT staff members of the requirements for full compliance with the records retention schedules. As discussed in Chapter 3, if adversaries in legal proceedings can demonstrate that employees are not adhering to approved records retention policies, the entire program comes into jeopardy, with document destruction being challenged as spoilage of evidence.

---

**SOFTWARE APPLICATIONS RECORDS RETENTION REQUIREMENTS**

**PURPOSE / SCOPE:** This policy provides requirements pertaining to records retention for company records residing in software applications. It provides requirements for incorporating functionality within those applications sufficient to comply with the company’s Records Retention Schedules.

**BACKGROUND:** ABC Corp. desires to retain only such records and information as are needed to operate its businesses and comply with the law. This fundamental principle is embodied in the...
company’s Records Retention Schedules. These retention schedules apply to records in all media formats—paper, photographic, and electronic. Many software applications, however, lack the requisite functionality to fulfill these retention or life cycle management requirements. This policy is prepared to provide guidance for incorporating these requirements into electronic recordkeeping environments.

SOFTWARE APPLICATIONS SUBJECT TO THIS POLICY: All internally developed computer programs, as well as software packages acquired from external sources must comply with the information life cycle requirements contained herein. These programs include production applications that frequently reside in legacy computing environments managed by the Information Technology (IT) Department. They also include desktop computer applications used by individuals, such as word processors, spreadsheets, and databases, as well as, network-based communications and workgroup applications such as electronic mail.

RESPONSIBILITIES:

Enterprise Records Retention Committee

Under its mandate to exercise general management oversight of ABC’s enterprise records management program, this committee has overall management responsibility for this policy and compliance with it, to include granting any exceptions with its requirements. Upon request of the committee, the Information Technology Department, the Records Management Department, and all software managers and developers are responsible for reporting compliance with this policy.

Information Technology Department

As maintainers of ABC’s computer hardware, software, and networks, and as managers of the technology infrastructure, the IT Department is responsible for ensuring that information life cycle management issues are properly addressed in all deployments of computer software within the company. More specifically, IT is responsible for the following:

- Working with the Records Management Department and with all company departments and business units to ensure that data purge functionality or other life cycle management capabilities are incorporated into all installed software in a manner that ensures compliance with the Records Retention Schedules.

- Working with the Tax Department to ensure full compliance with the provisions of IRS Revenue Procedure 98-25. This procedure prescribes requirements for retaining electronic records that are subject to tax audits by the Internal Revenue Service.

Records Management Department

Under its mandate for promoting sound records retention and information life cycle management throughout the company, this department is responsible for ensuring that all company departments and business units are familiar with the requirements discussed herein and for reporting the status of compliance with the policy to the Enterprise Records Retention Committee.

Software Developers / Managers

All programmers, systems analysts, business process modelers, database administrators, network specialists, and other technical personnel who acquire, develop, or otherwise manage software within ABC Corp. are directly responsible for implementing the life cycle management requirements discussed herein.

Compliance Requirements: All New Software and Existing Software Applications
All developers and managers of software applications are required to review the records residing in all applications for which they are responsible. They must identify retention requirements for those records as specified by the Records Retention Schedules and determine each software application’s functionality for compliance with those retention requirements. If the software lacks appropriate functionality, measures must be taken to implement it, as follows:

- **New Software.** All new software, whether internally developed or acquired from external sources, must comply with the requirements of this policy. No new software will be installed unless the requisite life cycle management requirements have been properly addressed and complied with.

- **Existing / Installed Software.** In cases where installed software applications lack the requisite life cycle management functionality to properly comply with the records retention schedules, software developers and managers are responsible for incorporating such functionality as soon as practicable, but not later than when each system application requiring such functionality is converted / upgraded to a new hardware and software environment.

### Data Retention Functionality Requirements

When software applications are developed or purchased, the following issues must be addressed to assure that appropriate records retention capabilities are incorporated into those applications:

1. Each software application must provide a method for defining retention requirements for all records created and maintained by that application.
2. Each software application must provide a method for determining destruction (deletion) dates for specific electronic records based on retention periods in the Records Retention Schedules.
3. Each software application must provide a method for identifying electronic records eligible for destruction when their retention periods have elapsed.
4. Each software application must provide the capability to override automatic deletion when litigation holds or tax holds are placed on electronic records. Further, the software must be able to remove such holds when authorized.
5. Each software application must be able to mark electronic records for deletion and provide a list of such records for approval by business owners or other parties prior to dele-

NOTES


2. This sample policy was assembled from project work on various consulting engagements in which the authors have participated during the past several years. We are particularly indebted to Dr. William Saffady for developing the responsibilities and compliance requirements sections of this policy during the course of one such engagement.

3. Ibid., “Applying Records Retention to Electronic Records.”
A P P E N D I X

Sampling of National Laws and Regulations of Electronic Records Retention from Australia, Canada, and the United States

Internal Revenue Service, Revenue Procedure 98–25 88
Code of Federal Regulations, National Archives and Records Administration 94
DoD 5015.2-STD, Design Criteria Standard for Electronic Records Management Software Applications 100
Electronic Signatures in Global and National Commerce Act 117
Uniform Electronic Transactions Act 124
United States Code – Government Paperwork Elimination Act 147
Revenue Canada 151
Australian Tax Office 156
National Archives and Records Administration 163
  General Records Schedule 20 163
  General Records Schedule 24, Information Technology Operations and Management Records; Proposed 167
  Expanding Transfer Options for Electronic Records 174
The purpose of this revenue procedure is to specify the basic requirements that the Internal Revenue Service considers to be essential in cases where a taxpayer's records are maintained within an Automatic Data Processing system (ADP). This revenue procedure updates and supersedes Rev. Proc. 91-59, 1991-2 C.B. 841.

SECTION 2. BACKGROUND

(1) The requirements of this revenue procedure pertain to all matters under the jurisdiction of the Commissioner of Internal Revenue including, but not limited to, income, excise, employment, and estate and gift taxes, as well as employee plans and exempt organizations.

(2) The requirements of this revenue procedure are applicable to any sections of the Code that have unique or specific recordkeeping requirements. For example, machine-sensible records maintained by the taxpayer to meet the requirements of section 274(d) relating to the amount, time, place, and business purpose of a business expense must meet the requirements of this revenue procedure.

(3) Except as otherwise provided in this revenue procedure, all requirements of section 6001 that apply to hardcopy books and records apply as well to machine-sensible books and records that are maintained within an ADP system.

SECTION 1. PURPOSE

The purpose of this revenue procedure is to specify the basic requirements that the Internal Revenue Service considers to be essential in cases where a taxpayer's records are maintained within an Automatic Data Processing system (ADP). This revenue procedure updates and supersedes Rev. Proc. 91-59, 1991-2 C.B. 841.

SECTION 2. BACKGROUND

(1) A taxpayer with assets of $10 million or more at the end of its taxable year must comply with the record retention requirements of Rev. Rul. 71-20 and the provisions of this revenue procedure. For purposes of this revenue procedure, a controlled group of corporations, as defined in section 1563, is considered to be one corporation and all assets of all members of the group are aggregated.

(2) A taxpayer with assets of less than $10 million at the end of its taxable year must comply with the record retention requirements of Rev. Rul. 71-20 and the provisions of this revenue procedure if any of the following conditions exists:

(a) all or part of the information required by section 6001 is not in the taxpayer's hardcopy books and records, but is available in machine-sensible data media used for recording, consolidating, and summarizing accounting transactions and records within a taxpayer's ADP system are records within the meaning of section 6001 and section 1.6001-1, and are required to be retained so long as the contents may become material in the administration of any internal revenue law.

SECTION 3. SCOPE

(1) The requirements of this revenue procedure pertain to all matters under the jurisdiction of the Commissioner of Internal Revenue including, but not limited to, income, excise, employment, and estate and gift taxes, as well as employee plans and exempt organizations.

(2) The requirements of this revenue procedure are applicable to any sections of the Code that have unique or specific recordkeeping requirements. For example, machine-sensible records maintained by the taxpayer to meet the requirements of section 274(d) relating to the amount, time, place, and business purpose of a business expense must meet the requirements of this revenue procedure.

(3) Except as otherwise provided in this revenue procedure, all requirements of section 6001 that apply to hardcopy books and records apply as well to machine-sensible books and records that are maintained within an ADP system.

SECTION 4. DEFINITIONS

.01 Section 6001 provides that every person liable for any tax imposed by the Code, or for the collection thereof, must keep such records, render such statements, make such returns, and comply with such rules and regulations as the Secretary may from time to time prescribe. Whenever necessary, the Secretary may require any person, by notice served upon that person or by regulations, to make such returns, render such statements, or keep such records, as the Secretary deems sufficient to show whether or not that person is liable for tax.

.02 Section 1.6001-1(a) of the Income Tax Regulations generally provides that persons subject to income tax, or required to file a return of information with respect to income, must keep such books or records, including inventories, as are sufficient to establish the amount of gross income, deductions, credits, or other matters required to be shown by that person in any return of such tax or information.

.03 Section 1.6001-1(e) provides that the books or records required by section 6001 must be kept available at all times for inspection by authorized internal revenue officers or employees, and must be retained so long as the contents thereof may become material in the administration of any internal revenue law.

.04 Rev. Rul. 71-20, 1971-1 C.B. 392, establishes that all machine-sensible data media used for recording, consolidating, and summarizing accounting transactions and records within a taxpayer's ADP system are records within the meaning of section 6001 and section 1.6001-1, and are required to be retained so long as the contents may become material in the administration of any internal revenue law.

SECTION 5. RETAINING MACHINE-SENSIBLE RECORDS

.01 Records.
(c) the taxpayer is notified by the District Director that machine-sensible records must be retained to meet the requirements of section 6001.

(3) A Controlled Foreign Corporation (CFC), a domestic corporation that is 25 percent foreign-owned, and a foreign corporation engaged in a trade or business within the United States at any time during a taxable year that maintains machine-sensible records within an ADP system must comply with the requirements of this revenue procedure to satisfy the recordkeeping requirements of sections 964(c), 982(d), 6038A(c)(4), and 6038C (and the regulations thereunder).

(4) An insurance company that maintains machine-sensible records within an ADP system to determine losses incurred under section 832(b)(5) must comply with the requirements of this revenue procedure and Rev. Proc. 75-56, 1975-2 C.B. 596. For this purpose, the machine-sensible records for a particular taxable year include the records for that year and the seven preceding years, all of which must be retained so long as they may become material to the examination of an insurance company’s federal tax return.

(5) A taxpayer’s use of a third party (such as a service bureau, time-sharing service, value-added network, or other third-party service) to provide services (e.g., custodial or management services) in respect of machine-sensible records does not relieve the taxpayer of its recordkeeping obligations and responsibilities under section 6001 and this revenue procedure.

SECTION 4. DEFINITIONS

.01 An “ADP system” consists of an accounting and/or financial system (and subsystems) that processes all or part of a taxpayer’s transactions, records, or data by other than manual methods. An ADP system includes, but is not limited to, a mainframe computer system, stand-alone or networked microcomputer system, Database Management System (DBMS), and a system that uses or incorporates Electronic Data Interchange (EDI) technology or an electronic storage system.

.02 “Capable of being processed” means the ability to retrieve, manipulate, print on paper (hardcopy), and produce output on electronic media. This term does not encompass any requirement that the program or system that created the computer data be available to process the data unless that program or system is necessary to:

(1) a tax-related computation (e.g., LIFO inventories, insurance company loss reserve computations, and foreign tax credit computations); or

(2) the retrieval of data (e.g., some database systems processes where the taxpayer chooses not to create a sequential extract (see section 5.02 of this revenue procedure)).

.03 A “DBMS” is a software system that creates, controls, relates, retrieves, and provides accessibility to data stored in a database.

.04 “EDI technology” is the computer-to-computer exchange of business information.

.05 An “electronic storage system” is a system used to prepare, record, transfer, index, store, preserve, retrieve, and reproduce books and records by either: (1) electronically imaging hardcopy documents to an electronic storage media; or (2) transferring computerized books and records to an electronic storage media using a technique such as “COLD” (computer output to laser disk), which allows books and records to be viewed or reproduced without the use of the original program. See Rev. Proc. 97-22, 1997-13 I.R.B. 9, for electronic storage system requirements.

.06 A “machine-sensible record” is data in an electronic format that is intended for use by a computer. Machine-sensible records do not include paper records or paper records that have been converted to an electronic storage medium such as microfilm, microfiche, optical disk, or laser disk.

SECTION 5. RETAINING MACHINE-SENSIBLE RECORDS

.01 General.

(1) The taxpayer must retain machine-sensible records so long as their contents may become material to the administration of the internal revenue laws under section 1.6001-1(e). At a minimum, this materiality continues until the expiration of the period of limitation for assessment, including extensions, for each tax year. In certain situations, records should be kept for a longer period of time. For example, records that pertain to fixed assets, losses incurred under section 832(b)(5), and LIFO inventories should be kept for longer periods of time.

(2) The taxpayer’s machine-sensible records must provide sufficient information to support and verify entries made on the taxpayer’s return and to determine the correct tax liability. The taxpayer’s machine-sensible records will meet this requirement only if they reconcile with the taxpayer’s books and the taxpayer’s return. A taxpayer establishes this reconciliation by demonstrating the relationship (i.e., audit trail):

(a) between the total of the amounts in the taxpayer’s machine-sensible records by account and the account totals in the taxpayer’s books; and

(b) between the total of the amounts in the taxpayer’s machine-sensible records by account and the taxpayer’s return.

(3) The taxpayer must ensure that its machine-sensible records contain sufficient transaction-level detail so that the information and the source documents underlying the machine-sensible records can be identified.

(4) All machine-sensible records required to be retained by this revenue procedure must be made available to the Service upon request and must be capable of being processed.

(5) Except as otherwise required by sections 5.01(2) or (3) of this revenue procedure, a taxpayer is not required to cre-
ate any machine-sensible record other than that created either in the ordinary course of its business or to establish return entries. For example, a taxpayer who does not create, in the ordinary course of its business, the electronic equivalent of a traditional paper document (such as an invoice) is not required by this revenue procedure to construct such a record, provided that the requirements of sections 5.01(2) and (3) are met. For requirements relating to hardcopy records, see section 11 of this revenue procedure. (6) A taxpayer’s disposition of a subsidiary company does not relieve the taxpayer of its responsibilities under this revenue procedure. The files and documentation retained for the Service by, or for, a disposed subsidiary must be retained as otherwise required by this revenue procedure.

.02 DBMS.

(1) A taxpayer has the discretion to create files solely for the use of the Service. For example, a taxpayer that uses a DBMS may satisfy the provisions of this revenue procedure by creating and retaining a sequential file that contains the transaction-level detail from the DBMS and otherwise meets the requirements of this revenue procedure. (2) A taxpayer that creates a file described in section 5.02(1) of this revenue procedure must document the process that created the sequential file in order to establish the relationship between the file created and the original DBMS records.

.03 EDI.

(1) A taxpayer that uses EDI technology must retain machine-sensible records that alone, or in combination with any other records (e.g., underlying contracts, price lists, and price changes), contain all the information that section 6001 requires of hardcopy books and records. For example, a taxpayer that uses EDI technology receives electronic invoices from its suppliers. The taxpayer decides to retain the invoice data from completed and verified EDI transactions in its accounts payable system rather than retain the incoming EDI transactions. Neither the EDI transactions, nor the accounts payable system, contain product descriptions or vendor names. To satisfy the requirements of section 6001, the taxpayer must supplement its EDI records with product code description lists and a vendor master file. (2) A taxpayer may capture the required detail for an EDI transaction at any level within its accounting system. However, the taxpayer must establish audit trails between the retained records and the taxpayer’s books, and between the retained records and the tax return. (3) Section 11.02 of this revenue procedure provides additional guidance concerning hardcopy requirements related to EDI transactions.

SECTION 6. DOCUMENTATION

.01 The taxpayer must maintain and make available to the Service upon request documentation of the business processes that:

(1) create the retained records;
(2) modify and maintain its records;
(3) satisfy the requirement of section 5.01(2) of this revenue procedure to support and verify entries made on the taxpayer’s return and determine the correct tax liability; and
(4) evidence the authenticity and integrity of the taxpayer’s records.

.02 The documentation described in section 6.01 of this revenue procedure must be sufficiently detailed to identify:

(1) the functions being performed as they relate to the flow of data through the system;
(2) the internal controls used to ensure accurate and reliable processing;
(3) the internal controls used to prevent the unauthorized addition, alteration, or deletion of retained records; and
(4) the charts of accounts and detailed account descriptions.

.03 With respect to each file that is retained, the taxpayer must maintain, and make available to the Service upon request, documentation of:

(1) record formats or layouts;
(2) field definitions (including the meaning of all “codes” used to represent information);
(3) file descriptions (e.g., data set name);
(4) evidence that periodic checks (described in section 9.01(3) of this revenue procedure) of the retained records were performed to meet section 9.02(1) of this revenue procedure, if the taxpayer wants to take advantage of section 9.02 of this revenue procedure;
(5) evidence that the retained records reconcile to the taxpayer’s books; and
(6) evidence that the retained records reconcile to the taxpayer’s tax return.

.04 The system documentation must include any changes to the items specified in sections 6.01, 6.02, and 6.03 of this revenue procedure and the dates these changes are implemented.

SECTION 7. RESOURCES

.01 The taxpayer must provide the Service at the time of an examination with the resources (e.g., appropriate hardware and software, terminal access, computer time, personnel, etc.) that the District Director determines is necessary to process the taxpayer’s machine-sensible books and records. At the request of the taxpayer, the District Director may, at the District Director’s discretion:

(1) identify the taxpayer’s resources that are not necessary to process books and records;
(2) allow a taxpayer to convert machine-sensible records to a different medium (e.g., from mainframe files to microcomputer diskette(s)).
(3) allow the taxpayer to satisfy the processing needs of the Service during off-peak hours; and
(4) allow the taxpayer to provide the Service with third-party equipment.

.02 An ADP system must not be subject, in whole or in part, to any agreement (such as a contract or license) that would limit or restrict the Service's access to and use of the ADP system on the taxpayer's premises (or any other place where the ADP system is maintained), including personnel, hardware, software, files, indexes, and software documentation.

SECTION 8. NOTIFICATION

.01 Except as provided in section 9.02 of this revenue procedure, the taxpayer must promptly notify its District Director if any machine-sensible records are lost, stolen, destroyed, damaged, or otherwise no longer capable of being processed (as defined in section 4.02 of this revenue procedure), or are found to be incomplete or materially inaccurate (affected records).

.02 The taxpayer's notice must identify the affected records and include a plan that describes how, and in what timeframe, the taxpayer proposes to replace or restore the affected records in a way that assures that they will be capable of being processed. The plan must demonstrate that all of the requirements of this revenue procedure will continue to be met with respect to the affected records.

.03 The District Director will notify the taxpayer of any objection(s) to the taxpayer's plan.

.04 A District Director may consider, whenever warranted by the facts and circumstances, the possibility of requiring less than a total restoration of missing data.

.05 Examples.

(1) Taxpayer A replaces its general ledger software system with a new general ledger software system with which the original system's records are incompatible. However, A's original records are retrievable and capable of being processed on A's hardware system. A is not required to notify its District Director of the change in its software system because A's records remain capable of being processed.

(2) Taxpayer B replaces its original ADP hardware system with a new system that cannot process the machine-sensible records created and maintained by B's original system. B must notify its District Director of this hardware system change and propose a plan for assuring that the machine-sensible records created and maintained by the original ADP hardware system are capable of being processed. To that end, B considers the following options: (1) having all records in the taxpayer's original system immediately reformatted so that the new system can retrieve and process those records; (2) having all records in its original system reformatted by a designated future date; or (3) having an arrangement with a third party to process all records in its original system on a compatible system. Any of these options may be acceptable provided the option selected enables the taxpayer to meet the requirements of this revenue procedure with respect to those records. The taxpayer must be able to demonstrate that any third party reformatting or processing is done with the quality controls in place that will ensure the continued integrity, accuracy, and reliability of the taxpayer's records.

SECTION 9. MAINTENANCE

.01 Recommended Practices.

(1) The implementation of records management practices is a business decision that is solely within the discretion of the taxpayer. Recommended records management practices include the labeling of records, providing a secure storage environment, creating back-up copies, selecting an offsite storage location, and testing to confirm records integrity.

(2) The National Archives and Records Administration's (NARA) Standards for the Creation, Use, Preservation, and Disposition of Electronic Records, 36 C.F.R., Ch. XII, Part 1234, Subpart C (1996), is one example of a records management resource that a taxpayer may choose to consult when formulating its records management practices.

(3) The NARA standard in 36 C.F.R. section 1234.30(g)(4) (1996) requires an annual reading of a statistical sampling of magnetic computer tape reels to identify any loss of data and to discover and correct the causes of data loss. In libraries with 1,800 or fewer storage units (e.g., magnetic tape reels), a 20 percent random sampling or a sample size of 50 units, whichever is larger, should be read. In libraries with more than 1,800 units, a sample of 384 units should be read. Although this NARA sampling standard is specifically for magnetic computer tape, the Service recommends that all retained machine-sensible records be sampled and tested as described in the NARA standard.

.02 Partial Loss of Data.

A taxpayer that loses only a portion of the data from a particular storage unit will not be subject to the penalties described in section 12 of this revenue procedure if the taxpayer can demonstrate to the satisfaction of the District Director that the taxpayer's data maintenance practices conform with 36 C.F.R. section 1234.30(g)(4) (1996) (the NARA sampling standard). However, the taxpayer remains responsible for substantiating the information on its return as required by section 6001.

SECTION 10. DISTRICT DIRECTOR AUTHORITY

.01 Record Retention Limitation Agreement.

(1) A taxpayer who maintains machine-sensible records may request to enter into a Record Retention Limitation Agreement (RRLA) with its District Director. This agree-
ment provides for the establishment and maintenance of records as agreed upon by the District Director and the taxpayer.

(2) The taxpayer’s request must identify and describe those records the taxpayer proposes not to retain and explain why those records will not become material to the administration of any internal revenue law. The District Director will notify the taxpayer whether or not the District Director will enter into an RRLA.

(3) In an RRLA, the District Director may waive all or any of the specific requirements in this revenue procedure. A taxpayer remains subject to all the requirements in this revenue procedure that are not specifically modified or waived by an RRLA.

(4) Unless an RRLA otherwise specifies, an RRLA shall not apply to accounting and tax systems added subsequent to the completion of the record evaluation upon which the agreement is based. All machine-sensible records produced by a subsequently added accounting and tax system, the contents of which may or may become material in the administration of the Code must be retained by the taxpayer signing the RRLA until a new evaluation is conducted by the District Director.

(5) Unless an RRLA specifies otherwise, it does not apply to a subsidiary acquired subsequent to the completion of the record evaluation upon which the RRLA is based. All machine-sensible records produced by the acquired subsidiary, the contents of which may become material in the administration of the Code must be retained pursuant to this revenue procedure and any pre-acquisition RRLA (“former RRLA”) that applies to the acquired subsidiary. The former RRLA applies to the acquired subsidiary until the District Director either revokes the former RRLA (in whole or in part) or enters into a new RRLA that applies to the acquired subsidiary.

(6) Upon the disposition of a subsidiary, the files being retained for the Service pursuant to an RRLA by, or for, the disposed subsidiary must be retained by the taxpayer until a new evaluation is conducted by the District Director.

(7) A District Director’s decision to revoke an RRLA, or not to enter into an RRLA, does not relieve the taxpayer of its recordkeeping obligations under section 6001 or its responsibilities described in this revenue procedure.

.02 Records Evaluation.

(1) The District Director may conduct a records evaluation at any time the District Director deems it appropriate to review the taxpayer’s record retention practices, including the taxpayer’s relevant data processing and accounting systems.

(2) The records evaluation described in section 10.02(1) of this revenue procedure is not an “examination,” “investigation,” or “inspection” of the books and records within the meaning of section 7605(b) of the Code, or a prior audit for purposes of section 530 of the Revenue Act of 1978, 1978-3 (Vol. 1) C.B. 119, as amended by section 1122 of the Small Business Job Protection Act of 1996, because this evaluation is not directly related to the determination of the tax liability of a taxpayer for a particular taxable period.

(3) The District Director will inform the taxpayer of the results of a records evaluation.

.03 Testing.

(1) The District Director may periodically initiate tests to establish the authenticity, readability, completeness, and integrity of a taxpayer’s machine-sensible records retained in conformity with this revenue procedure.

(2) These tests may include a review of integrated systems such as EDI or an electronic storage system, and a review of the internal controls and security procedures associated with the creation and maintenance of the taxpayer’s records.

(3) The tests described in section 10.03(1) of this revenue procedure are not an “examination,” “investigation,” or “inspection” of the books and records within the meaning of section 7605(b) of the Code, or a prior audit for purposes of section 530 of the Revenue Act of 1978, 1978-3 (Vol. 1) C.B. 119, as amended by section 1122 of the Small Business Job Protection Act of 1996, because these tests are not directly related to the determination of the tax liability of a taxpayer for a particular taxable period.

(4) The District Director will inform the taxpayer of the results of these tests.

SECTION 11. HARDCOPY RECORDS

.01 The provisions of this revenue procedure do not relieve taxpayers of their responsibility to retain hardcopy records that are created or received in the ordinary course of business as required by existing law and regulations. Hardcopy records may be retained in microfiche or microfilm format in conformity with Rev. Proc. 81-46, 1981-2 C.B. 621. Hardcopy records may also be retained in an electronic storage system in conformity with Rev. Proc. 97-22. These records are not a substitute for the machine-sensible records required to be retained by this revenue procedure.

.02 A taxpayer need not create or retain hardcopy records if:

(1) the hardcopy records are merely computer printouts created only for validation, control, or other temporary purposes;

(2) the hardcopy records are not produced in the ordinary course of transacting business (as may be the case when utilizing EDI technology); or

(3) all the details relating to the transaction are subsequently received by the taxpayer in an EDI transaction and are retained as machine-sensible records by the taxpayer in conformity with this revenue procedure. For example, a taxpayer need not retain credit card receipts generated at the time of a transaction if all pertinent
information on the receipts is subsequently received in an EDI transaction and retained as a machine-sensible record. See section 5.03 of this revenue procedure for requirements relating to EDI.

.03 A taxpayer need not create hardcopy printouts of its machine-sensible records unless requested to do so by the Service. The Service may request such hardcopy printouts either at the time of an examination or in conjunction with the tests described in section 10.03(1) of this revenue procedure.

SECTION 12. PENALTIES

The District Director may issue a Notice of Inadequate Records pursuant to section 1.6001-1(d) if a taxpayer fails to comply with this revenue procedure (including a failure to satisfy the resource requirements of section 7 of this revenue procedure). Failure to comply with this revenue procedure may also result in the imposition of the applicable penalties under subtitle F of the Code, including the section 6662(a) accuracy-related civil penalty and the section 7203 willful failure criminal penalty.

SECTION 13. EFFECT ON OTHER DOCUMENTS

Rev. Proc. 91-59 is modified and superseded for machine-sensible records relating to taxable years beginning after December 31, 1997. However, a taxpayer that complies with this revenue procedure for taxable years beginning prior to that date is treated as having complied with Rev. Proc. 91-59 for those years.

SECTION 14. EFFECTIVE DATE

This revenue procedure is effective for machine-sensible records relating to taxable years beginning after December 31, 1997.

SECTION 15. INTERNAL REVENUE SERVICE OFFICE CONTACT

.01 Questions regarding this revenue procedure should be directed to the Office of the Assistant Commissioner (Examination). The telephone number for this office is (202)622-5480 (not a toll-free number). Written questions should be addressed to: Assistant Commissioner (Examination) Attention: CP:EX

Internal Revenue Service
1111 Constitution Ave., NW
Washington, DC 20224

.02 Questions regarding the application of this revenue procedure to a specific factual situation should be directed to the appropriate District Director’s office.

SECTION 16. PAPERWORK REDUCTION ACT

The collections of information contained in this revenue procedure have been reviewed and approved by the Office of Management and Budget in accordance with the Paperwork Reduction Act (44 U.S.C. 3507) under control number 1545-1595.

An agency may not conduct or sponsor, and a person is not required to respond to, a collection of information unless the collection of information displays a valid control number.

The collections of information in this revenue procedure are in sections 8 and 10 of this revenue procedure. This information is required to ensure that machine-sensible records will constitute records within the meaning of section 6001. The collections of information are mandatory for a taxpayer whose machine-sensible records are kept within an ADP system. The likely respondents are individuals, state or local governments, farms, business or other for-profit institutions, federal agencies or employees, nonprofit institutions, and small businesses or organizations.

The estimated total annual recordkeeping burden is 120,000 hours.

The estimated annual burden per recordkeeper will vary from 20 hours to 60 hours, depending on individual circumstances, with an estimated average of 40 hours. The estimated number of recordkeepers is 3,000.

Books or records relating to a collection of information must be retained as long as their contents may become material in the administration of any internal revenue law. Generally tax returns and tax return information are confidential, as required by 26 U.S.C. 6103.
1234.1 Scope of part. 
This part establishes the basic requirements related to the creation, maintenance, use, and disposition of electronic records. Electronic records include numeric, graphic, and text information, which may be recorded on any medium capable of being read by a computer and which satisfies the definition of a record. This includes, but is not limited to, magnetic media, such as tapes and disks, and optical disks. Unless otherwise noted, these requirements apply to all electronic information systems, whether on microcomputers, minicomputers, or main-frame computers, regardless of storage media, in network or stand-alone configurations. This part also covers creation, maintenance and use, and disposition of Federal records created by individuals using electronic mail applications.

1234.2 Definitions. 
Basic records management terms are defined in 36 CFR 1220.14. As used in part 1234 —

Database means a set of data, consisting of at least one data file that is sufficient for a given purpose.

Data file means related numeric, textual, or graphic information that is organized in a strictly prescribed form and format.

Electronic information system. A system that contains and provides access to computerized Federal records and other information.

Electronic mail message. A document created or received on an electronic mail system including brief notes, more formal or substantive narrative documents, and any attachments, such as word processing and other electronic documents, which may be transmitted with the message.

Electronic mail system. A computer application used to create, receive, and transmit messages and other documents. Excluded from this definition are file transfer utilities (software that transfers files between users but does not retain any transmission data), data systems used to collect and process data that have been organized into data files or databases on either personal computers or mainframe computers, and word processing documents not transmitted on an e-mail system.

Electronic record means any information that is recorded in a form that only a computer can process and that satisfies the definition of a Federal record in 44 U.S.C. 3301.

Electronic recordkeeping system. An electronic system in which records are collected, organized, and categorized to facilitate their preservation, retrieval, use, and disposition.

Text documents means narrative or tabular documents, such as letters, memorandums, and reports, in loosely prescribed form and format.

Transmission and receipt data.

(1) Transmission data. Information in electronic mail systems regarding the identities of sender and addressee(s), and the date and time messages were sent.

(2) Receipt data. Information in electronic mail systems regarding date and time of receipt of a message, and/or acknowledgment of receipt or access by addressee(s).

Appendix – Code of Federal Regulations

§1234.22 Creation and use of text documents.

(a) Electronic recordkeeping systems that maintain the official file copy of text documents on electronic media shall meet the following minimum requirements:

(1) Provide a method for all authorized users of the system to retrieve desired documents, such as an indexing or text search system;

(2) Provide an appropriate level of security to ensure integrity of the documents;

(3) Provide a standard interchange format when necessary to permit the exchange of documents on electronic media among agency computers using different software/operating systems.

(b) Agencies shall maintain adequate and up-to-date technical documentation for each electronic information system that produces, uses, or stores data files. Minimum documentation required is a narrative description of the system; physical and technical characteristics of the records, including a record layout that describes each field and the relationship between data elements in databases; and any other technical information needed to read or process the records.

§1234.20 Creation and use of data files.

(a) For electronic information systems that produce, use, or store data files, disposition instructions for the data shall be incorporated into the system's design.

(b) Agencies shall maintain adequate and up-to-date technical documentation for each electronic information system that produces, uses, or stores data files. Minimum documentation required is a narrative description of the system; physical and technical characteristics of the records, including a record layout that describes each field and the relationship between data elements in databases; and any other technical information needed to read or process the records.


Subpart C — Standards for the Creation, Use, Preservation, and Disposition of Electronic Records

Appendix – Code of Federal Regulations

§1234.20 Creation and use of data files.

(a) For electronic information systems that produce, use, or store data files, disposition instructions for the data shall be incorporated into the system's design.

(b) Agencies shall maintain adequate and up-to-date technical documentation for each electronic information system that produces, uses, or stores data files. Minimum documentation required is a narrative description of the system; physical and technical characteristics of the records, including a record layout that describes each field and the relationship between data elements in databases; and any other technical information needed to read or process the records.

ing systems and the conversion or migration of documents on electronic media from one system to another; and

(4) Provide for the disposition of the documents including, when necessary, the requirements for transferring permanent records to NARA (see §1228.270 of this chapter).

(b) Before a document is created electronically on electronic recordkeeping systems that will maintain the official file copy on electronic media, each document shall be identified sufficiently to enable authorized personnel to retrieve, protect, and carry out the disposition of documents in the system. Appropriate identifying information for each document maintained on the electronic media may include: office of origin, file code, key words for retrieval, addressee (if any), signator, author, date, authorized disposition (coded or otherwise), and security classification (if applicable). Agencies shall ensure that records maintained in such systems can be correlated with related records on paper, microform, or other media.


§1234.24 Standards for managing electronic mail records.

Agencies shall manage records created or received on electronic mail systems in accordance with the provisions of this chapter pertaining to adequacy of documentation, recordkeeping requirements, agency records management responsibilities, and records disposition (36 CFR parts 1220, 1222, and 1228).

(a) Agency instructions on identifying and preserving electronic mail messages will address the following unique aspects of electronic mail:

(1) Some transmission data (names of sender and addressee(s) and date the message was sent) must be preserved for each electronic mail record in order for the context of the message to be understood. Agencies shall determine if any other transmission data is needed for purposes of context.

(2) Agencies that use an electronic mail system that identifies users by codes or nicknames or identifies addressees only by the name of a distribution list shall instruct staff on how to retain names on directories or distributions lists to ensure identification of the sender and addressee(s) of messages that are records.

(3) Agencies that use an electronic mail system that allows users to request acknowledgments or receipts showing that a message reached the mailbox or inbox of each addressee, or that an addressee opened the message, shall issue instructions to e-mail users specifying when to request such receipts or acknowledgments for recordkeeping purposes and how to preserve them.

(4) Agencies with access to external electronic mail systems shall ensure that Federal records sent or received on these systems are preserved in the appropriate recordkeeping system and that reasonable steps are taken to capture available transmission and receipt data needed by the agency for recordkeeping purposes.

(5) Some e-mail systems provide calendars and task lists for users. These may meet the definition of Federal record. Calendars that meet the definition of Federal records are to be managed in accordance with the provisions of General Records Schedule 23, Item 5.

(6) Draft documents that are circulated on electronic mail systems may be records if they meet the criteria specified in 36 CFR 1222.34.

(b) Agencies shall consider the following criteria when developing procedures for the maintenance of electronic mail records in appropriate recordkeeping systems, regardless of format.

(1) Recordkeeping systems that include electronic mail messages must:

(i) Provide for the grouping of related records into classifications according to the nature of the business purposes the records serve;

(ii) Permit easy and timely retrieval of both individual records and files or other groupings of related records;

(iii) Retain the records in a usable format for their required retention period as specified by a NARA-approved records schedule;

(iv) Be accessible by individuals who have a business need for information in the system;

(v) Preserve the transmission and receipt data specified in agency instructions; and

(vi) Permit transfer of permanent records to the National Archives and Records Administration (see 36 CFR 1228.270 and 36 CFR 1234.32(a)).

(2) Agencies shall not store the recordkeeping copy of electronic mail messages that are Federal records only on the electronic mail system, unless the system has all of the features specified in paragraph (b)(1) of this section. If the electronic mail system is not designed to be a recordkeeping system, agencies shall instruct staff on how to copy Federal records from the electronic mail system to a recordkeeping system.

(c) Agencies that maintain their electronic mail records electronically shall move or copy them to a separate electronic recordkeeping system unless their system has the features specified in paragraph (b)(1) of this section. Because they do not have the features specified in paragraph (b)(1) of this section, backup tapes should not be used for recordkeeping purposes. Agencies may retain records from electronic mail systems in an off-line electronic storage format (such as optical disk or magnetic tape) that meets the requirements described at 36 CFR 1234.30(a). Agencies that retain permanent electronic mail records scheduled for transfer to the National Archives shall either store them in a format and on a medium that conforms to the requirements concerning transfer at 36 CFR 1228.188 or shall maintain the ability to convert the records to the required format and medium at the time transfer is scheduled.
Agencies that maintain paper files as their record-keeping systems shall print their electronic mail records and the related transmission and receipt data specified by the agency.


§1234.26 Judicial use of electronic records.

Electronic records may be admitted in evidence to Federal courts for use in court proceedings (Federal Rules of Evidence 803(8)) if trustworthiness is established by thoroughly documenting the recordkeeping system's operation and the controls imposed upon it. Agencies should implement the following procedures to enhance the legal admissibility of electronic records.

(a) Document that similar kinds of records generated and stored electronically are created by the same processes each time and have a standardized retrieval approach.

(b) Substantiate that security procedures prevent unauthorized addition, modification, or deletion of a record and ensure system protection against such problems as power interruptions.

(c) Identify the electronic media on which records are stored throughout their life cycle, the maximum time span that records remain on each storage medium, and the NARA-approved disposition of all records.

(d) Coordinate all of the above with legal counsel and senior IRM and records management staff.


§1234.28 Security of electronic records.

Agencies shall implement and maintain an effective records security program that incorporates the following:

(a) Ensures that only authorized personnel have access to electronic records.

(b) Provides for backup and recovery of records to protect against information loss.

(c) Ensures that appropriate agency personnel are trained to safeguard sensitive or classified electronic records.

(d) Minimizes the risk of unauthorized alteration or erasure of electronic records.

(e) Ensures that electronic records security is included in computer systems security plans prepared pursuant to the Computer Security Act of 1987 (40 U.S.C. 759 note).


§1234.30 Selection and maintenance of electronic records storage media.

(a) Agencies shall select appropriate media and systems for storing agency records throughout their life, which meet the following requirements:

(1) Permit easy retrieval in a timely fashion;

(2) Facilitate distinction between record and nonrecord material;

(3) Retain the records in a usable format until their authorized disposition date; and

(4) If the media contains permanent records and does not meet the requirements for transferring permanent records to NARA as outlined in §1228.270 of this chapter, permit the migration of the permanent records at the time of transfer to a medium which does meet the requirements.

(b) The following factors shall be considered before selecting a storage medium or converting from one medium to another:

(1) The authorized life of the records, as determined during the scheduling process;

(2) The maintenance necessary to retain the records;

(3) The cost of storing and retrieving the records;

(4) The records density;

(5) The access time to retrieve stored records;

(6) The portability of the medium (that is, selecting a medium that will run on equipment offered by multiple manufacturers) and the ability to transfer the information from one medium to another (such as from optical disk to magnetic tape); and

(7) Whether the medium meets current applicable Federal Information Processing Standards.

(c) Agencies should avoid the use of floppy disks for the exclusive long-term storage of permanent or unscheduled electronic records.

(d) Agencies shall ensure that all authorized users can identify and retrieve information stored on diskettes, removable disks, or tapes by establishing or adopting procedures for external labeling.

(e) Agencies shall ensure that information is not lost because of changing technology or deterioration by converting storage media to provide compatibility with the agency’s current hardware and software. Before conversion to a different medium, agencies must determine that the authorized disposition of the electronic records can be implemented after conversion.

(f) Agencies shall back up electronic records on a regular basis to safeguard against the loss of information due to equipment malfunctions or human error. Duplicate copies of permanent or unscheduled records shall be maintained in storage areas separate from the location of the records that have been copied.

(g) Maintenance of magnetic computer tape. (1) Agencies shall test magnetic computer tapes no more than 6 months prior to using them to store electronic records.
that are unscheduled or scheduled for permanent retention. This test should verify that the tape is free of permanent errors and in compliance with National Institute of Standards and Technology or industry standards.

(2) Agencies shall maintain the storage and test areas for computer magnetic tapes containing permanent and unscheduled records at the following temperatures and relative humidities:

Constant temperature — 62 to 68°F.

Constant relative humidity — 35% to 45%

(3) Agencies shall annually read a statistical sample of all reels of magnetic computer tape containing permanent and unscheduled records to identify any loss of data and to discover and correct the causes of data loss. In tape libraries with 1800 or fewer reels, a 20% sample or a sample size of 50 reels, whichever is larger, should be read. In tape libraries with more than 1800 reels, a sample of 384 reels should be read. Tapes with 10 or more errors should be replaced and, when possible, lost data shall be restored. All other tapes which might have been affected by the same cause (i.e., poor quality tape, high usage, poor environment, improper handling) shall be read and corrected as appropriate.

(4) Agencies shall copy permanent or unscheduled data on magnetic tapes before the tapes are 10 years old onto tested and verified new tapes.

(5) External labels (or the equivalent automated tape management system) for magnetic tapes used to store permanent or unscheduled electronic records shall provide unique identification for each reel, including the name of the organizational unit responsible for the data, system title, and security classification, if applicable. Additionally, the following information shall be maintained for (but not necessarily attached to) each reel used to store permanent or unscheduled electronic records: file title(s); dates of creation; dates of coverage; the recording density; type of internal labels; volume serial number, if applicable; number of tracks; character code/software dependency; information about block size; and reel sequence number, if the file is part of a multi-reel set. For numeric data files, include record format and logical record length, if applicable; number of records; and number of records for each data set.

(6) Agencies shall prohibit smoking and eating in magnetic computer tape storage libraries and test or evaluation areas that contain permanent or unscheduled records.

(h) Maintenance of direct access storage media. (1) Agencies shall issue written procedures for the care and handling of direct access storage media which draw upon the recommendations of the manufacturers.

(2) External labels for diskettes or removable disks used when processing or temporarily storing permanent or unscheduled records shall include the following information: name of the organizational unit responsible for the records, descriptive title of the contents, dates of creation, security classification, if applicable, and identification of the software and hardware used.


§1234.32 Retention and disposition of electronic records.

Agencies shall establish policies and procedures to ensure that electronic records and their documentation are retained as long as needed by the Government. These retention procedures shall include provisions for:

(a) Scheduling the disposition of all electronic records, as well as related documentation and indexes, by applying General Records Schedules (particularly GRS 20 or GRS 23) as appropriate or submitting an SF 115, Request for Records Disposition Authority, to NARA (see part 1228 of this chapter). The information in electronic information systems, including those operated for the Government by a contractor, shall be scheduled as soon as possible but no later than one year after implementation of the system.

(b) Transferring a copy of the electronic records and any related documentation and indexes to the National Archives at the time specified in the records disposition schedule in accordance with instructions found in §1228.270 of this chapter. Transfer may take place at an earlier date if convenient for both the agency and the National Archives and Records Administration.

(c) Establishing procedures for regular recopying, reformatting, and other necessary maintenance to ensure the retention and usability of electronic records throughout their authorized life cycle (see §1234.28).

(d) Electronic mail records may not be deleted or otherwise disposed of without prior disposition authority from NARA (44 U.S.C. 3303a). This applies to the original version of the record that is sent or received on the electronic mail system and any copies that have been transferred to a recordkeeping system. See 36 CFR part 1228 for records disposition requirements.

(1) Disposition of records on the electronic mail system. When an agency has taken the necessary steps to retain the record in a recordkeeping system, the identical version that remains on the user’s screen or in the user’s mailbox has no continuing value. Therefore, NARA has authorized deletion of the version of the record on the electronic mail system under General Records Schedule 20, Item 14, after the record has been preserved in a recordkeeping system along with all appropriate transmission data.

(2) Records in recordkeeping systems. The disposition of electronic mail records that have been transferred to an appropriate recordkeeping system is governed by the records schedule or schedules that control the records in that system. If the records in the system are not scheduled, the agency shall follow the procedures at 36 CFR part 1228.
§1234.34 Destruction of electronic records.

Electronic records may be destroyed only in accordance with a records disposition schedule approved by the Archivist of the United States, including General Records Schedules. At a minimum each agency shall ensure that:

(a) Electronic records scheduled for destruction are disposed of in a manner that ensures protection of any sensitive, proprietary, or national security information.

(b) Magnetic recording media previously used for electronic records containing sensitive, proprietary, or national security information are not reused if the previously recorded information can be compromised by reuse in any way.

(c) Agencies shall establish and implement procedures that specifically address the destruction of electronic records generated by individuals employing electronic mail.

This Standard is reissued under the authority of DoD Directive 5015.2, “Department of Defense Records Management Program,” March 6, 2000, which provides implementing and procedural guidance on the management of records in the Department of Defense. It sets forth mandatory baseline functional requirements for Records Management Application (RMA) software used by the DoD Components in the implementation of their records management programs; defines required system interfaces and search criteria to be supported by the RMAs; and describes the minimum records management requirements that must be met, based on current National Archives and Records Administration (NARA) regulations.


This Standard applies to the Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the Department of Defense (hereafter referred to collectively as “the DoD Components”).

This Standard is effective immediately and is mandatory for use by all DoD Components. Electronic records management information systems already in use must comply with this Standard within 2 years of the effective date of this document. The Heads of the DoD Components may issue supplementary instructions only when necessary to provide for unique requirements within their organizations provided that those instructions do not adversely affect interoperability and compatibility with DoD Automated Information Systems (AISs).

Send recommended changes to:
Department of Defense
Voice: 703-607-0510
Office of DASD (Deputy CIO)
FAX: 703-607-0248
Architecture & Interoperability Directorate
1931 Jefferson Davis Highway
Crystal Mall-3, 7th Floor
DSN: 224-0510
E-mail: michael.todd@osd.mil

This Standard is approved for public release; distribution is unlimited. The DoD Components, other Federal Agencies, and the public may obtain copies of this Standard via Internet at http://www.dtic.mil/whs/directives.

JOHN P. STENBIT
Assistant Secretary of Defense for Command, Control, Communications and Intelligence
C1.1. PURPOSE

This Standard sets forth mandatory baseline functional requirements, and identifies nonmandatory features deemed desirable for Records Management Application (RMA) software. This revised version of the standard incorporates requirements for classified marking, access control, declassification and downgrading, and other issues. The Department of Defense (DoD) Components will use this Standard in the implementation of their records management programs. This standard describes the minimum records management requirements that must be met in accordance with 44 U.S.C. 2902 (reference (o)) and guidance and implementing regulations promulgated by the National Archives and Records Administration (NARA). Also, the word “shall” identifies mandatory system standards and the word “should” identifies design objectives that are desirable but not mandatory.

C1.2. LIMITATIONS

This Standard addresses a minimum set of baseline functional requirements applicable to all RMAs used within the Department of Defense. For the Defense Information Systems Agency’s (DISA) Joint Interoperability Test Command (JITC) to certify that an RMA is compliant with this Standard, these minimum requirements must be met, regardless of organizational and site-specific needs. Using organizations may identify additional requirements to satisfy their site-specific needs, but these functions will not be certified as compliant by JITC. Some examples of site-specific needs are the capability to label Privacy Act data and data exempt from release under the Freedom of Information Act (FOIA), and the capability of adopting features described as optional in Chapter 3 of this Standard. These requirements will be addressed in a later version of this Standard. Additionally, future versions of this Standard will address interface with the Defense Message System (DMS), the incorporation of standard data elements, and interoperability within the organization’s enterprise information environment, and among disparate RMAs.

C2. CHAPTER 2 – MANDATORY REQUIREMENTS

C2.1. GENERAL REQUIREMENTS

C2.1.1. Managing Records. RMAs shall manage records in accordance with this Standard, regardless of storage media or other characteristics (see 44 U.S.C. 3103 and 36 CFR 1222.10, references (p) and (q)).

C2.1.2. Accommodating Dates and Date Logic. RMAs shall correctly accommodate and process information that contains dates in current, previous, and future centuries (see FIPS 4-2, reference (r)). The capability shall include, but not be limited to, century recognition, calculation, and logic that accommodates same century and multicentury formulas and date values, and date interface values that reflect the century. RMAs shall store years in a 4-digit format. Leap year calculations shall be accommodated (e.g., 1900 is not a leap year; 2000 is a leap year).

C2.1.3. Implementing Standard Data. RMAs shall allow for the implementation of standardized data in accordance with DoD 8320.1-M (reference (s)). When selecting commercial-off-the-shelf (COTS) products to support RMA requirements, selection criteria should include the feasibility and capability of the COTS products to implement and maintain DoD data standards. This requirement implies the capability for adding user-defined metadata fields and modifying existing field labels.

C2.1.4. Backward Compatibility. RMAs shall provide the capability to access information from their superseded repositories and databases. This capability shall support at least one previously verified version of backward compatibility.

C2.1.5. Accessibility. The available documentation for RMAs shall include product information that describes features that address 36 CFR parts 1194.21 and 1194.31 (references (t) and (u)). For web-based applications, 36 CFR part 1194.22 (reference (v)) shall also apply (see 29 U.S.C. 794d, reference (w)).

C2.2. DETAILED REQUIREMENTS

C2.2.1. Implementing File Plans.

C2.2.1.1. RMAs shall provide the capability for only authorized individuals to create, edit, and delete file plan components and their identifiers. Each component identifier shall be linked to its associated component and to its higher-level component identifier(s) (see 44 U.S.C. 3303 and 36 CFR 1222.50, references (x) and (y)). Mandatory file plan components are shown in Table C2.T.1. Mandatory in the Structure column indicates that the field must be present and available to the user either as read/write or as read only depending upon the kind of data being stored. Mandatory in the Data Collection Required by User column indicates that RMAs shall ensure population of the associated data structure withnonnull values. For fields that are not mandatory in the Data Collection column, RMAs shall behave in a predictable manner as a result of queries or other operations when the fields are not populated. The file plan components should be organized into logical sets that, when populated, will provide all the file plan references necessary to properly annotate (file) a record.

C2.2.1.2. RMAs shall provide the capability for authorized individuals to designate the metadata fields that are to be constrained to selection lists. RMAs shall provide the capability for authorized individuals to create and
maintain selection lists (e.g., drop-down lists) for metadata items that are constrained to a predefined set of data.

C2.2.1.3. RMAs shall provide the capability for only authorized individuals to create, edit, and delete record folder components and their identifiers. Each component identifier shall be linked to its associated component and to its higher-level file plan component identifier(s) (see references (t) and (y)). Mandatory record folder components are shown in Table C2.T2. Mandatory in the Structure column indicates that the field shall be present and available to the user either as read/write or as read only depending upon the kind of data being stored. Mandatory in the Data Collection Required by User column indicates that RMAs shall ensure population of the associated data structure with nonnull values. For fields that are not mandatory in the Data Collection column, RMAs shall behave in a predictable manner as a result of queries or other operations when the fields are not populated.

C2.2.1.4. RMAs shall ensure that identifiers (e.g., folder identifiers, record category identifiers) are unique so that ambiguous assignments, links, or associations cannot occur.

C2.2.1.5. RMAs shall provide the capability to allow only an authorized individual to define and attach user-defined business rules and/or access logic to any metadata field including user-defined fields.

C2.2.1.6. RMAs shall provide the capability to sort, view, save, and print user-selected portions of the file plan, including record folders (see reference (z)).

C2.2.2. Scheduling Records.

C2.2.2.1. RMAs shall provide the capability for only authorized individuals to view, create, edit, and delete disposition schedule components of record categories.

C2.2.2.2. RMAs shall provide the capability for defining multiple phases (e.g., transfer to inactive on-site storage, transfer to off-site storage) within a disposition schedule.

C2.2.2.3. RMAs shall provide the capability for only authorized individuals to define the cutoff criteria and, for each life cycle phase, the following disposition components for a record category:

C2.2.2.3.1. Retention Period (e.g., fiscal year).

C2.2.2.3.2. Disposition Action (interim transfer, accession, permanent, or destroy).

C2.2.2.3.3. Interim Transfer or Accession Location (if applicable).

C2.2.2.4. RMAs shall, as a minimum, be capable of scheduling and rescheduling each of the following three types of cutoff and disposition instructions (see reference (d)).

### Table C2.T1. File Plan Components

<table>
<thead>
<tr>
<th>Requirement</th>
<th>File Plan Component</th>
<th>Structure</th>
<th>Data Collection Required by User</th>
<th>Reference/Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>C2.1.1.</td>
<td>Record Category Name</td>
<td>Mandatory</td>
<td>Mandatory</td>
<td>RMTF (reference (z))</td>
</tr>
<tr>
<td>C2.1.2.</td>
<td>Record Category Identifier</td>
<td>Mandatory</td>
<td>Mandatory, RMAs shall ensure unique</td>
<td>RMTF (reference (z))</td>
</tr>
<tr>
<td>C2.1.3.</td>
<td>Record Category Description</td>
<td>Mandatory</td>
<td>Mandatory</td>
<td>RMTF (reference (z))</td>
</tr>
<tr>
<td>C2.1.4.</td>
<td>Disposition Instructions</td>
<td>Mandatory</td>
<td>Mandatory</td>
<td>36 CFR 1228.24 (reference)</td>
</tr>
<tr>
<td>C2.1.5.</td>
<td>Disposition Authority</td>
<td>Mandatory</td>
<td>Mandatory</td>
<td>RMTF (reference (z))</td>
</tr>
<tr>
<td>C2.1.6.</td>
<td>Permanent Record Indicator</td>
<td>Mandatory</td>
<td>Mandatory</td>
<td></td>
</tr>
<tr>
<td>C2.1.7.</td>
<td>Vital Record Indicator</td>
<td>Mandatory</td>
<td>Mandatory</td>
<td>36 CFR 1236.20 (reference)</td>
</tr>
<tr>
<td>C2.1.8.</td>
<td>Vital Record Review and Update Cycle Period</td>
<td>Mandatory, conditional on Vital Record Indicator</td>
<td>Mandatory, conditional on Vital Record Indicator</td>
<td>36 CFR 1236.20 reference (ab)</td>
</tr>
<tr>
<td>C2.1.9.</td>
<td>User Definable</td>
<td>Mandatory/Optional</td>
<td>Multiple user defined fields shall</td>
<td></td>
</tr>
</tbody>
</table>
C2.2.2.4.1. Time Dispositions, where records are eligible for disposition immediately after the conclusion of a fixed period of time following user-defined cutoff (e.g., days, months, years).

C2.2.2.4.2. Event Dispositions, where records are eligible for disposition immediately after a specified event takes place (i.e., event acts as cutoff and there is no retention period).

C2.2.2.4.3. Time-Event Dispositions, where the timed retention periods are triggered after a specified event takes place (i.e., event makes the record folder eligible for closing and/or cutoff and there is a retention period).

C2.2.2.5. RMAs shall provide the capability to automatically calculate the complete life cycle, including intermediate phases, of record folders and records not in folders (see reference (d)).

C2.2.2.6. RMAs shall provide the capability for rescheduling dispositions of record folders and/or records (those not in folders) during any phase of their life cycle if an authorized individual changes the disposition instructions. This requirement includes the capability to change the cutoff criteria of disposition instructions and to change the retention period associated with a disposition.

C2.2.2.7. The RMA shall provide recalculation of the record life cycle based on changes to any life-cycle date and set the filing status (i.e., open, closed) of the folder according to the business rules associated with date change(s).

C2.2.3. Declaring and Filing Records.

C2.2.3.1. RMAs shall provide the capability to associate the attributes of one or more record folder(s) to a record, or for categories to be managed at the record level, rather than at the folder level.

C2.2.3.2. Mandatory record metadata components are shown in Table C2.T3. Mandatory in the Structure column indicates that the field shall be present and available to the user either as read/write or as read-only depending upon the kind of data being stored. Mandatory in the Data Collection Required column indicates that RMAs shall ensure population of the associated data structure with nonnull values. For fields that are not mandatory in the Data Collection column, RMAs shall behave in a predictable manner as a result of queries or other operations when the fields are not populated.

C2.2.3.3. RMAs shall provide the capability for only authorized individuals to create, edit, and delete record metadata components, and their associated selection lists.

C2.2.3.4. RMAs shall provide the capability for authorized individuals to select where data collection for optional metadata fields is mandatory for a given organization.
C2.2.3.5. RMAs shall assign a unique computer-generated record identifier for each record they manage regardless of where that record is stored (see reference (z)).

C2.2.3.6. RMAs shall provide the capability to create, view, save, and print the complete record metadata, or user-specified portions thereof, in user-selectable order (see reference (z)).

C2.2.3.7. RMAs shall provide the capability for authorized individuals to arrange record metadata components and user-defined record components on data entry screens to be used for filing.

C2.2.3.8. RMAs shall prevent subsequent changes to electronic records stored in its supported repositories. The content of the record, once filed, shall be preserved (see references (y) and (z)).

C2.2.3.9. RMAs shall not permit modification of the metadata fields indicated by this Standard as not editable.
C2.2.3.10. RMAs shall (for all records) capture, populate, and/or provide the user with the capability to populate the metadata elements before filing the record. RMAs shall ensure that fields designated mandatory for data collections arenonnull before filing the record (see references (y) and (ah)).

C2.2.3.11. For records that are being filed via the user interface, RMAs shall provide the user with the capability to edit the record metadata prior to filing the record, except for data specifically identified in this Standard as not editable. For autofiling, RMAs shall provide the user the option of editing the record metadata prior to filing.

C2.2.3.12. Dates captured electronically shall be valid dates as defined in paragraph C2.1.2. Where data entry/capture errors are detected, RMAs shall prompt the user to correct the error. These prompts shall provide guidance to the user in making corrective actions; for example, “Date format incorrect - use MM/DD/YYYY.”

C2.2.3.13. RMAs shall restrict the capability to only authorized individuals to define and add user-defined metadata fields (e.g., project number, budget line) for site-specific requirements (see reference (ah)).

C2.2.3.14. RMAs shall provide the capability to view, save, or print the metadata associated with a specified record or set of records, or user-specified portions thereof, in user-selectable order.

C2.2.3.15. RMAs shall provide the capability for only authorized individuals to limit the record folders and record categories presented to a user or workgroup. Based on these limits, RMAs shall present to users only those record categories or folders available to the user or workgroup for filing.

C2.2.3.16. RMAs shall provide the capability for only authorized individuals to change a record folder or record category associated with a record.

C2.2.3.17. RMAs shall provide a capability for referencing or linking and associating supporting and related records and related information, such as notes, marginalia, attachments, and electronic mail-return receipts, etc., to a specified record. RMAs shall allow only authorized individuals to change or delete links and associations (see reference (z)).

C2.2.3.18. RMAs shall provide the capability to link original superseded records to their successor records.

C2.2.3.19. RMAs shall provide the capability to support multiple renditions of a record. These shall be associated and linked.

C2.2.3.20. RMAs shall provide the capability to increment versions of records when filing. RMAs shall associate and link the versions.

C2.2.3.21. RMAs shall link the record metadata to the record so that it can be accessed for display, export, etc. (see 36 CFR 1234.32, reference (ai)).

C2.2.3.22. RMAs shall provide the capability for only authorized individuals to modify the metadata of stored records. However, RMAs shall not allow the editing of metadata fields that have been specifically identified in this Standard as not editable.

C2.2.3.23. RMAs shall enforce data integrity, referential integrity, and relational integrity.

C2.2.3.24. RMAs shall provide the capability to automatically synchronize multiple databases and repositories.

C2.2.3.25. RMAs shall provide the capability for users to create and maintain shortened “quick-pick” lists from the authorized lists.

C2.2.3.26. RMAs shall provide the capability for users to create and maintain templates that automatically populate commonly used data into record metadata fields.

C2.2.4. Filing Electronic Mail Messages (E-mail).

C2.2.4.1. RMAs shall treat e-mail messages the same as any other record, and these shall be subject to all requirements of this Standard (see 32 CFR 1222.32 and 36 CFR 1234.24, references (aj) and (ak)).

C2.2.4.2. RMAs shall capture and automatically store the transmission and receipt data identified in Table C2.T4 if available from the e-mail system, as part of the record metadata when an e-mail message is filed as a record (see reference (ak)). RMAs shall provide the capability for editing Subject or Title, Author or Originator, Addressee(s), and the Other Addressee(s) metadata fields prior to filing. All other fields shall not be editable.

C2.2.4.3. RMAs shall provide the user the option of filing e-mail and all its attachment(s) as a single record, or filing selected e-mail item(s) as individual record(s), or to do both. When the attachment(s) is (are) filed as individual record(s), the user shall be provided the capability to enter the metadata required in table C2.T3. (see reference (ak)).

C2.2.5. Storing Records.

C2.2.5.1. RMAs shall provide at least one portal that provides access to all associated repositories and databases storing electronic records and their metadata.

C2.2.5.2. The RMAs shall prevent unauthorized access to the repository(ies) (see 36 CFR 1222.50 and 44 U.S.C. 3105, references (y) and (al)).

C2.2.5.3. RMAs shall manage and preserve any record in any supported repository, regardless of its format or structure, so that, when retrieved, it can be reproduced, viewed, and manipulated in the same manner as the original (see references (y), (z), and (ah)).

C2.2.5.4. RMAs shall allow only authorized individuals to move or delete records from the repository (see 36 CFR 1222.50 and 36 CFR 1234.28, references (y) and (am)).
C2.2.6. Retention and Vital Records Management.

C2.2.6.1. Screening Records.

C2.2.6.1.1. RMAs shall provide for sorting, viewing, saving, and printing list(s) of record folders and/or records (regardless of media) based on any combination of the following:

C2.2.6.1.1.1. Disposition Action Date.
C2.2.6.1.1.2. Disposition Action.
C2.2.6.1.1.3. Location.
C2.2.6.1.1.4. Transfer or Accession Location.
C2.2.6.1.1.5. Vital Records Review and Update Cycle Period or Date.
C2.2.6.1.1.6. Record Category Identifier.
C2.2.6.1.1.7. Folder Unique Identifier.
C2.2.6.1.1.8. User Definable Fields.

C2.2.6.1.2. RMAs shall provide for sorting, viewing, saving, and printing life cycle information, eligibility dates, and events of user-selected record folders and records.

C2.2.6.1.3. RMAs shall allow the user to select and order the columns presented in the screening result list(s).

C2.2.6.1.4. RMAs shall provide authorized individuals with the capability to indicate when the specified event has occurred for records and record folders with event- and time-event-driven dispositions.

C2.2.6.1.5. RMAs shall provide for sorting, viewing, saving, and printing lists and partial lists of record folders and/or records that have no assigned disposition.

C2.2.6.2. Closing Record Folders.

C2.2.6.2.1. RMAs shall provide a capability for authorized individuals to close record folders to further filing after the specified event occurs.

C2.2.6.2.2. RMAs shall provide the capability only to authorized individuals to add records to a previously closed record folder or to reopen a previously closed record folder for additional public filing.

C2.2.6.3. Cutting Off Record Folders.

C2.2.6.3.1. RMAs shall be capable of implementing cut-off instructions for scheduled and unscheduled record folders. RMAs shall identify record folders eligible for cutoff, and present them only to the authorized individual for cutoff approval. The cutting off of a folder shall start the first phase of its life cycle controlled by the records schedule (see reference (z)).

C2.2.6.3.2. RMAs shall provide the capability to only authorized individuals to add records or make other alterations to record folders that have been cut off.

C2.2.6.4. Freezing/Unfreezing Records.

C2.2.6.4.1. RMAs shall provide the capability for only authorized individuals to extend or suspend (freeze) the retention period of record folders or records beyond their scheduled disposition (see 44 U.S.C. 2909 and 36 CFR 1228.54, references (an) and (ao)).

C2.2.6.4.2. RMAs shall provide a field for authorized individuals to enter the reason for freezing a record or record folder.

C2.2.6.4.3. RMAs shall identify record folders and/or records that have been frozen and provide authorized individuals with the capability to unfreeze them.

C2.2.6.4.4. RMAs shall allow authorized individuals to search, update, and view the reason for freezing a record or record folder.

C2.2.6.5. Transferring Records.
C2.2.6.5.1. RMAs shall identify and present those record folders and records eligible for interim transfer and/or accession (see references (p) and (z)).

C2.2.6.5.2. RMAs shall, for records approved for interim transfer or accession and that are stored in the RMA's supported repository(ies), copy the pertinent records and associated metadata of the records and their folders to a user-specified filename, path, or device. For permanent records to be accessioned to the National Archives, the accessioning file(s) shall be made to conform to one of the formats and media specified in 36 CFR 1228.2702 (see references (z), (ai), and (ap)). (See requirement C2.2.10.5.)

C2.2.6.5.3. RMAs shall, for records approved for accession and that are not stored in an RMA supported repository, copy the associated metadata for the records and their folders to a user-specified filename, path, or device. For permanent records to be accessioned to the National Archives, the metadata shall be made to conform to one of the formats and media specified in reference (ap).

C2.2.6.5.4. RMAs shall, for records approved for interim transfer or accession, provide the capability for only authorized individuals to delete the records and/or related metadata after successful transfer has been confirmed (see references (al) and (ao)). RMAs shall provide the capability to allow the organization to retain the metadata for records that were transferred or accessioned.

C2.2.6.5.5. RMAs shall provide documentation of transfer activities. This documentation shall be stored as records.

C2.2.6.6. Destroying Records.

C2.2.6.6.1. RMAs shall identify and present the record folders and records, including record metadata, that are eligible for destruction, as a result of reaching that phase in their life cycle. Records assigned more than one disposition must be retained and linked to the Record Folder (Category) with the longest retention period. Links to Record Folders (Categories) with shorter retention periods should be removed as they become due (see references (h), (z), and (ai)).

C2.2.6.6.2. RMAs shall, for records approved for destruction, present a second confirmation requiring authorized individuals to confirm the delete command, before the destruction operation is executed (see references (z) and (al)).

C2.2.6.6.3. RMAs shall delete electronic records approved for destruction in a manner such that the records cannot be physically reconstructed (see 36 CFR 1234.34, reference (aq)).

C2.2.6.6.4. RMAs shall provide an option allowing the organization to select whether to retain or delete the metadata of destroyed records.

C2.2.6.6.5. RMAs shall restrict the records destruction commands to authorized individuals (see references (y) and (al)).

C2.2.6.6.6. RMAs shall provide documentation of destruction activities. This documentation shall be stored as records.

C2.2.6.7. Cycling Vital Records.

C2.2.6.7.1. RMAs shall provide the capability for authorized individuals to enter the Vital Records Review and Update Cycle Period when creating or updating the file plan.

C2.2.6.7.2. RMAs shall provide the capability to enter the date when the records associated with a vital records folder have been reviewed and updated.

C2.2.6.7.3. RMAs shall provide a means for identifying and aggregating vital records due for cycling.

C2.2.6.7.4. RMAs shall provide a means for identifying and aggregating vital records by previous cycle dates.

C2.2.6.8. Searching for and Retrieving Records.

C2.2.6.8.1. RMAs shall allow users to browse the records stored in the file plan based on their user access permissions.

C2.2.6.8.2. RMAs shall allow searches using any combination of the record and/or folder metadata elements (see reference (z)).

C2.2.6.8.3. RMAs shall allow the user to specify partial matches and shall allow designation of “wild card” fields or characters.

C2.2.6.8.4. RMAs shall allow searches using Boolean and relational operators: “and,” “and not,” “or,” “greater than” (>), “less than” (<), “equal to” (=), and “not equal to” (<>), and provide a mechanism to override the default (standard) order of precedence.

C2.2.6.8.5. RMAs shall present the user a list of records and/or folders meeting the retrieval criteria, or notify the user if there are no records and/or folders meeting the retrieval criteria. RMAs shall allow the user to select and order the columns presented in the search results list for viewing, transmitting, printing, etc. (see reference (z)).

C2.2.6.8.6. RMAs shall allow users the ability to search for null or undefined values.

C2.2.6.8.7. RMAs shall provide to the user’s workspace (filename, location, or path name specified by the user) copies of electronic records, selected from the list of records meeting the retrieval criteria, in the format in which they were provided to the RMA for filing (see reference (z)).

C2.2.6.8.8. RMAs shall provide the capability for filed e-mail records to be retrieved back into a compatible e-mail application for viewing, forwarding, replying, and any other action within the capability of the e-mail application.

C2.2.6.8.9. When the user selects a record for retrieval, RMAs shall present a list of available versions, defaulting to the latest version of the record for retrieval, but allow the user to select and retrieve any version.
C2.2.6.8.10. RMAs shall allow users to select any number of records, and their metadata, for retrieval from the search results list.

C2.2.6.8.11. RMAs shall allow the user to abort a search.

C2.2.7. Access Controls. Table C2.T5. summarizes requirements that refer to “authorized individuals” and offers additional information regarding example user-type roles and responsibilities. In general, Application Administrators are responsible for setting up the RMA infrastructure. Records Managers are responsible for records management administration. Privileged Users are those who are given special permissions to perform functions beyond those of typical users. RMAs shall provide the capability to allow organizations to define roles and responsibilities to fit their records management operating procedures.

Table C2.T5. Authorized Individual Requirements

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Application Administrator</th>
<th>Records Manager</th>
<th>Privileged User</th>
</tr>
</thead>
<tbody>
<tr>
<td>C2.2.1.1. Create, edit, and delete file plan components and their identifiers.</td>
<td>Ensures that data structures are correctly installed and database links are in place</td>
<td>Enters file plan data</td>
<td>None</td>
</tr>
<tr>
<td>C2.2.1.2. Designate the metadata fields that are to be constrained to selection lists. Create and maintain selection lists (e.g., drop-down lists) for metadata items that are constrained to a predefined set of data.</td>
<td>Ensure database is correctly set up and installed</td>
<td>Define Lists</td>
<td>User abilities</td>
</tr>
<tr>
<td>C2.2.1.3. Create, edit, and delete record folder components and their identifiers.</td>
<td>Ensures that data structures are correctly installed and database links are in place</td>
<td>Enters folder data</td>
<td>Enters folder data</td>
</tr>
<tr>
<td>C2.2.1.5. Define and attach user-defined business rules and/or access logic to metadata fields including user-defined fields.</td>
<td>Creates rules and connects them to fields</td>
<td>Manually execute rules if necessary</td>
<td>None</td>
</tr>
<tr>
<td>C2.2.2.1. View, create, edit, and delete disposition schedule components of record categories.</td>
<td>Ensures that data structures are correctly installed and database links are in place</td>
<td>Enters disposition data, enters event data, closes folders</td>
<td>Enters event data and closes folders</td>
</tr>
<tr>
<td>C2.2.2.3. Define the cutoff criteria and, for each life cycle phase, the following disposition components for a record category. . .</td>
<td>Ensures that data structure is correctly installed and database links are in place</td>
<td>Enters criteria and database links are in place</td>
<td>None</td>
</tr>
<tr>
<td>C2.2.2.6. Change the disposition instructions.</td>
<td>None</td>
<td>Edits disposition information and manually executes rules necessary to reschedule</td>
<td>None</td>
</tr>
<tr>
<td>C2.2.3.3. Create, edit, and delete record metadata Selection Lists components, and their associated selection lists.</td>
<td>Enters data is correctly installed and database links are in place</td>
<td>Ensures that data structure</td>
<td>Creates (all users)</td>
</tr>
<tr>
<td>C2.2.3.4. Select where data collection for optional metadata fields is mandatory for a given organization.</td>
<td>During setup</td>
<td>Advising</td>
<td>None</td>
</tr>
<tr>
<td>C2.2.3.7. Arrange record metadata components and user-defined record components on data entry screens to be used for filing.</td>
<td>During setup</td>
<td>Advising</td>
<td>None</td>
</tr>
<tr>
<td>C2.2.3.13. Define and add user-defined metadata fields (e.g., project number, budget line) for site-specific requirements.</td>
<td>During setup</td>
<td>Advising</td>
<td>None</td>
</tr>
<tr>
<td>C2.2.3.15. Limit the record folders and record categories presented to a user or workgroup.</td>
<td>Record Categories during setup</td>
<td>Record Folders</td>
<td>Record Folders</td>
</tr>
<tr>
<td>C2.2.3.16. Change a record folder or record category associated with a record.</td>
<td>As necessary</td>
<td>As necessary</td>
<td>None</td>
</tr>
<tr>
<td>C2.2.3.17. Change or delete links and associations. Database is correctly installed and configured</td>
<td>Change links as necessary</td>
<td>Change links as necessary</td>
<td>Make links</td>
</tr>
<tr>
<td>C2.2.3.22. Modify the metadata of stored records. As necessary</td>
<td>Change data as necessary</td>
<td>Change data as necessary</td>
<td>As necessary</td>
</tr>
<tr>
<td>C2.2.5.3. Move or delete records from the repository.</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
</tbody>
</table>
C2.2.7.1. The RMA, in conjunction with its operating environment, shall use identification and authentication measures that allow only authorized persons access to the RMA. At a minimum, the RMA will implement identification and authentication measures that require the following (see EO 12958, DoD Directive 5200.28 and E.O. 12968, references (c), (ar), and (as)).

C2.2.7.1.1. User id.

C2.2.7.1.2. Password. (RMAs shall provide the capability for authorized users to define the minimum length of the Password field.)

C2.2.7.2. RMAs shall provide the capability for only individuals with Application Administrator access to authorize access capabilities to any combination of the items identified in Table C2.T5. to individuals and to groups.

C2.2.7.3. RMAs shall provide the capability to define different groups of users with different access privileges.

C2.2.7.1.3. Alternative methods, such as Biometrics, Common Access Cards (CAC), or Public Key Infrastructure (PKI), in lieu of or in conjunction with the above, are acceptable. If used in lieu of, the alternative must provide at least as much security.

C2.2.7.2. RMAs shall provide the capability for only individuals with Application Administrator access to authorize access capabilities to any combination of the items identified in Table C2.T5. to individuals and to groups.

C2.2.7.3. RMAs shall provide the capability to define different groups of users with different access privileges.

---

### Table C2.T5. Authorized Individual Requirements (continued)

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Application Administrator</th>
<th>Records Manager</th>
<th>Privileged User</th>
</tr>
</thead>
<tbody>
<tr>
<td>C2.2.6.1.4. Indicate when the specified event has occurred for records and record folders with event and time-event driven dispositions.</td>
<td>Database setup Link dispositions to record categories Enter event information</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C2.2.6.2.1. Close record folders to further filing after the specified event occurs.</td>
<td>As necessary As necessary As necessary</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C2.2.6.2.2. Add records to a previously closed record folder or to reopen a previously closed record folder for additional public filing.</td>
<td>As necessary As necessary As necessary</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C2.2.6.3.1. Approve cutoff.</td>
<td>As necessary Routine work None</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C2.2.6.3.2. Add records or make other alterations to record folders that have been cut off.</td>
<td>Database support Enters limits None</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C2.2.6.4.1. Extend or suspend (freeze) the retention Unfreezing period of record folders or records beyond their scheduled disposition.</td>
<td>None Database and business Freezing/</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C2.2.6.4.2. Enter the reason for freezing a record or record folder.</td>
<td>Database and business rules Freezing/ Unfreezing None</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C2.2.6.4.3. Unfreeze capability.</td>
<td>Database and business rules Freezing/ Unfreezing None</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C2.2.6.4.4. Search, update, and view the reason for freezing a record or record folder.</td>
<td>Database and business rules Freezing/ Unfreezing None</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C2.2.6.5.4. Delete the records and/or related metadata after successful transfer has been confirmed.</td>
<td>As necessary As necessary None</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C2.2.6.6.2. Confirm the delete command, before the destruction operation is executed.</td>
<td>As necessary As necessary None</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C2.2.6.6.5. Access to records destruction commands.</td>
<td>As necessary As necessary None</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C2.2.6.7.1. Enter the Vital Records Review and Update Cycle Period when creating or updating the file plan.</td>
<td>Ensuring database structure Enters cycling data Cycles and Records</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C2.2.7.1. Allow access to the RMA.</td>
<td>As necessary As necessary None</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C2.2.7.1.2. Define the minimum length of the Password field.</td>
<td>Define minimum length None None</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C2.2.8.2. Determine which of the objects and specified actions listed in subparagraph C2.2.8.1. are audited.</td>
<td>Manage audits None None</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C2.2.8.3. Set up specialized reports to . . .</td>
<td>Create reports None None</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C2.2.8.5. Export and/or backup and remove</td>
<td>Export and/or backup File audit logs as None</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
C2.2.8. System Audits.

C2.2.8.1. The RMA, in conjunction with its operating environment, shall provide an audit capability to log the actions, date, time, unique object identifier(s) and user identifier(s) for actions performed on the following RMA objects:

- C2.2.8.1.1. User Accounts.
- C2.2.8.1.2. User Groups.
- C2.2.8.1.3. Records.
- C2.2.8.1.4. Associated metadata elements.
- C2.2.8.1.5. File plan components.

These actions include retrieving, creating, deleting, searching, and editing actions (see references (c) and (ar)). Logging of searching and retrieving actions are not required for User Accounts and User Groups.

C2.2.8.2. The RMA shall provide a capability whereby only authorized individuals can determine which of the objects and specified actions listed in subparagraph C2.2.8.1. are audited (see reference (c)).

C2.2.8.3. The RMA, in conjunction with its operating environment, shall provide audit analysis functionality whereby an authorized individual can set up specialized reports to:

- C2.2.8.3.1. Determine what level of access a user has and to track a user’s actions. These are the specified actions listed in subparagraph C2.2.8.1 (see references (c) and (z)).
- C2.2.8.3.2. Facilitate reconstruction, review, and examination of the events surrounding or leading to mishandling of records, possible compromise of sensitive information, or denial of service.

C2.2.8.4. RMAs shall provide the capability to file the audit data as a record (see reference (z)).

C2.2.8.5. The RMA, in conjunction with its operating environment, shall allow only authorized individuals to export and/or back up and remove audit files from the system.

C2.2.8.6. The RMA, in conjunction with its operating environment, shall not allow audit logs to be edited.

C2.2.9. System Management Requirements. The following functions are typically provided by the operating system or by a database management system. These functions are also considered requirements to ensure the integrity and protection of organizational records. They shall be implemented as part of the overall records management system even though they may be performed externally to an RMA.

C2.2.9.1. Backup of Stored Records. The RMA system shall provide the capability to automatically create back-up or redundant copies of the records and their metadata (see references (z), (ag) and (am)).

C2.2.9.2. Storage of Back-up Copies. The method used to back up RMA database files shall provide copies of the records and their metadata that can be stored off-line and at separate location(s) to safeguard against loss due to system failure, operator error, natural disaster, or willful destruction (see 36 CFR 1234.30, reference (at)).

C2.2.9.3. Recovery/Rollback Capability. Following any system failure, the back-up and recovery procedures provided by the system shall:

- C2.2.9.3.1. Ensure data integrity by providing the capability to compile updates (records, metadata, and any other information required to access the records) to RMAs.
- C2.2.9.3.2. Ensure these updates are reflected in RMA files, and ensuring that any partial updates to RMA files are separately identified. Also, any user whose updates are incompletely recovered, shall, upon next use of the application, be notified that a recovery has been attempted. RMAs shall also provide the option to continue processing using all in-progress data not reflected in RMA files (see references (z) and (am)).
- C2.2.9.3.4. Rebuild Capability. The system shall provide the capability to rebuild from any back-up copy, using the back-up copy and all subsequent system audit trails (see reference (z)).

C2.2.9.5. Storage Availability and Monitoring. The system shall provide for the monitoring of available storage space. The storage statistics shall provide a detailed accounting of the amount of storage consumed by RMA processes, data, and records. The system shall notify individuals of the need for corrective action in the event of critically low storage space (see reference (z)).

C2.2.9.6. Safeguarding. The RMA, in conjunction with its operating environment, shall have the capability to activate a keyboard lockout feature and a screen-blanking feature (see reference (c)).

C2.2.10. Additional Baseline Requirements. Following are records management requirements that shall be implemented by the organization, but not necessarily by the RMAs.

C2.2.10.1. Electronic Calendars and Task Lists. Some electronic systems provide calendars and task lists for
users. These may meet NARA’s definition of a record (see reference (j)). Calendars and task lists that meet the definition of records shall be managed as any other record. If the RMA being acquired does not have the capability to extract calendars and task lists from the software application that generates them, the user organization shall implement processes or procedures to enable those records to be managed by the RMA.

C2.2.10.2. External E-mail. Some organizations use separate e-mail systems for Internet e-mail or other wide area network e-mail. These records shall be handled as any other e-mail records. If the RMA being acquired does not provide the capabilities specified in paragraph C2.2.3., the user organization shall implement processes or procedures to enable these records to be managed by the RMA (see reference (ak)).

C2.2.10.3. Ability to Read and Process Records. Since RMAs are prohibited (see subparagraph C2.2.3.8.) from altering the format of stored records, the organization shall ensure that it has the ability to view, copy, print, and, if appropriate, process any record stored in RMAs for as long as that record must be retained. The organization may meet this requirement by:

C2.2.10.3.1. Maintaining the hardware and software used to create or capture the record.

C2.2.10.3.2. Maintaining hardware and software capable of viewing the record in its native format.

C2.2.10.3.3. Ensuring backward-compatibility when hardware and software is updated, or:

C2.2.10.3.4. Migrating the record to a new format before the old format becomes obsolete. Any migration shall be pre-planned and controlled to ensure continued reliability of the record (see reference (at)).

C2.2.10.4. Distribution Lists. If the RMA is unable to access and store e-mail distribution lists from the e-mail server, the organization shall implement procedures to extract and store them as records.

C2.2.10.5. Accessioning Records to NARA. When accessioning records and metadata to NARA, if conforming to formats and media specified in 36 CFR 1228.270 (reference (ap)) causes a violation of the records’ authenticity and/or integrity, the organization shall contact NARA for guidance.

C2.2.10.6. Applying Records Disposition Schedule to Back-up Copies. The using organization shall schedule the back-up copies and recycle or destroy the medium in accordance with the disposition schedule.

C3. CHAPTER 3 – NONMANDATORY FEATURES

C3.1. REQUIREMENTS DEFINED BY THE ACQUIRING OR USING ACTIVITY

In addition to the baseline requirements defined by this Standard, the acquiring or using activity should identify the following Agency-, site-, and installation-unique requirements. These requirements are not mandatory for DoD compliance.

C3.1.1. Storage Availability. The acquiring or using activity should define the size of the storage space required for its organizational records, along with the related record metadata and associated audit files.

C3.1.2. Documentation. The acquiring or using activity should define the type and format of desired documentation, such as user guides, technical manuals, and installation procedures, to be provided by the vendor.

C3.1.3. System Performance. The acquiring or using activity should specify what constitutes acceptable RMA system availability, reliability, response times, and downtimes that will satisfy its business requirements.

C3.1.4. Hardware Environment. The acquiring or using activity should define the hardware environment (for example, mainframe, client-server, or personal computer) and identify the platforms (servers and workstations) on which the RMA is to run.

C3.1.5. Operating System Environment. The acquiring or using activity should define the operating system environment (for example, UNIX, Windows, Linux, Macintosh) on which the RMA is to be run.

C3.1.6. Network Environment. The acquiring or using activity should define the Local Area Network (LAN), Wide Area Network (WAN) or other network topology (e.g., Ethernet bus, star, or token-ring) and the Network Operating System (NOS) (e.g., Novell, Banyan Vines, Windows NT Server) on which the RMA is to run.

C3.1.7. Protocols. The acquiring or using activity should identify the protocols, such as Transmission Control Protocol/Internet Protocol (TCP/IP), Simple Mail Transfer Protocol (SMTP), or X.400 that the RMA is to support.

C3.1.8. Electronic Mail Interface. The acquiring or using activity should specify the e-mail application(s) with which the RMA is to interface.

C3.1.9. End-User Orientation and Training. The acquiring or using activity should specify records manager and end-user training requirements.

C3.2. OTHER USEFUL RMA FEATURES

Many RMA products provide the following time and labor-saving functions, either as standard or optional features to enhance the utility of the system (the acquiring or using activity should determine local requirements for any of the following RMA features).

C3.2.1. Making Global Changes. RMAs should provide the capability for authorized individuals to make global changes to the record category names, record category identifiers, disposition components, and originating organization. In addition, RMAs should provide the
capability to reorganize the file plan and automatically propagate the changes resulting from the reorganization to the affected records and record folders.

C3.2.2. Bulk Loading Capability. RMAs should provide the capability for authorized individuals to bulk load:

C3.2.2.1. An Agency’s pre-existing file plan.
C3.2.2.2. Electronic records.
C3.2.2.3. Record metadata.

C3.2.3. Interfaces to Other Software Applications. RMAs should interface with various office automation packages such as electronic mail, word processors, spreadsheets, databases, desktop publishers, and electronic data interchange systems, as specified by the using activity.

C3.2.4. Report Writer Capability. RMAs should provide the capability to generate reports on the information held within the RMA’s repository based upon user-developed report templates or user queries.

C3.2.5. On-Line Help. RMAs should have an on-line help capability for access to user operational information. Help should be context sensitive to the screens from which help was launched. Global help should be available from a toolbar menu item or hot key.

C3.2.6. Document Imaging Tools. RMAs should be capable of interfacing with document imaging and workflow software and hardware. These should be consistent with the DoD Automated Document Conversion Master Plan.

C3.2.7. Fax Integration Tools. An organization may determine a need for RMAs to interface with desktop or server-based fax products to capture fax records in their electronic format.

C3.2.8. Bar Code Systems. An organization may determine a need for RMAs to use a bar code system with RMAs. The following examples show how bar code technology can be used to support records management tasks:

C3.2.8.1. File and correspondence tracking to positions, sections, or staff members.
C3.2.8.2. Creating, printing, and reading labels for non-electronic records.
C3.2.8.3. Boxing records for transfer.
C3.2.8.4. Box tracking for records-holding facility operations.
C3.2.8.5. Workflow tracking.
C3.2.8.6. Posting changes in disposition.
C3.2.8.7. Recording audit and census functions.
C3.2.9. Retrieval Assistance. RMAs should have additional search and retrieval features, such as full text search, to assist the user in locating records. The search utility should include the capability to create, modify, or import additional thesauri.

C3.2.10. File Plan Component Selection/Search Capability. RMAs should provide methods for assisting the user in the selection of the file plan components to be assigned to a record, such as priority-ordered lists or directed searches.

C3.2.11. Workflow and/or Document Management Features. An organization may determine that RMAs should have the capability to manage working and draft versions of documents and other potential record materials as they are being developed.

C3.2.12. Records Management Forms and Other Forms. An organization may determine that RMAs should be capable of interfacing with forms generating software and/or have the capability to generate completed standard records management forms, such as:

C3.2.12.3. Standard Form 258, “Agreement To Transfer Records To The National Archives Of The United States.”
C3.2.12.4. National Archives Form 14012, “Database Record Layout.”
C3.2.12.5. National Archives Form 14097, “Technical Description for Transfer of Electronic Records to the National Archives.”
C3.2.13. Printed Labels. RMAs should provide the capability to produce hard-copy codes or identifiers in the form of labels or other products, as required.
C3.2.14. Viewer. RMAs should provide the capability to view each file in its stored format or a human-readable rendition.
C3.2.15. Web Capability. RMAs should provide the capability to allow the user to interface through a web browser or other platform independent means.
C3.2.16. Government Information Locator Service. RMAs should have the capability to implement the requirements of the Government Information Locator Service (GILS) (see reference (m)). GILS was established to identify public information resources throughout the Federal Government, describe the information available in those resources, and provide assistance in obtaining this information.
C3.2.17. Enhanced Support for Off-line Records. RMAs should provide additional features for managing boxes of hard-copy records and other off-line archives.
C4. CHAPTER 4 – MANAGEMENT OF CLASSIFIED RECORDS

C4.1. REQUIREMENTS FOR RMAs SUPPORTING MANAGEMENT OF CLASSIFIED RECORDS

The following requirements address the management of classified records. As such, these requirements are only mandatory for those RMAs that manage classified records. These requirements are in addition to those requirements outlined in Chapters 2 and 3. In this chapter, the word “shall” identifies mandatory system standards for vendors who support the management of classified records. The word “should” identifies design objectives that are desirable but not mandatory for supporting classified records management. Additionally, requirements for safeguarding and providing security for classified records are not in the scope of this document, since they are provided in other more applicable directives and regulations.

C4.1.1. Mandatory Metadata Fields for Classified Records. RMAs shall provide a capability by which a user can add metadata that describes a classified record. These metadata elements are shown in Table C4.T1. (see references (c) and (au)). Mandatory in the Structure column indicates that the field shall be present and available to the user either as read/write or as read-only depending upon the kind of data being stored. Mandatory in the Data Collection Required by User column indicates that RMAs shall ensure population of the associated data structure with nonnull values. For fields that are not mandatory in the Data Collection column, RMAs shall behave in a predictable manner as a result of queries or other operations when the fields are not populated.

Table C4.T1. Classified Record Components

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Component</th>
<th>Structure</th>
<th>Data Collection Required by User</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>C4.T1.1.1. 1.3, DoD References</td>
<td>Initial Classification</td>
<td>Mandatory</td>
<td>Mandatory, Option List is user expandable and must include: Confidential, Secret, Top Secret, No Markings</td>
<td>EO 12958: Sec. 1.1(d), Sec. 1.7 (a)(1) and (e); and 5200.1-R: Appendix F (references (c) and (ag))</td>
</tr>
<tr>
<td>C4.T1.2. 1.3, DoD References</td>
<td>Current Classification</td>
<td>Mandatory</td>
<td>Mandatory, Option List is user expandable and must include: Confidential, Secret, Top Secret, No Markings</td>
<td>EO 12958: Sec. 1.1(d), Sec. 1.7 (a)(1) and (e); and 5200.1-R: Appendix F (references (c) and (ag))</td>
</tr>
<tr>
<td>C4.T1.3. 32 CFR 2001.22(c)</td>
<td>Reason(s) For Classification</td>
<td>Mandatory</td>
<td>Mandatory</td>
<td>EO 12958: Sec. 1.7(a)(5); and CFR 2001: Subsection 2001.21(a)(3) and Subsection (references (c) and (au))</td>
</tr>
<tr>
<td>C4.T1.4.</td>
<td>Classified By</td>
<td>Mandatory</td>
<td>Mandatory if no data in Derived From, otherwise default</td>
<td>EO 12958: Sec. 1.4 and Sec. 1.7(a)(2) and (3); and 32 CFR 2001.21(a)(1) and (2) (references (c) and (au))</td>
</tr>
<tr>
<td>C4.T1.5. and</td>
<td>Derived From</td>
<td>Mandatory</td>
<td>Mandatory if no data in Classified By, otherwise default</td>
<td>EO 12958: Sec. 2.1 and 2.2; 32 CFR 2001.22(a) and (b) (references (c) and (au))</td>
</tr>
<tr>
<td>C4.T1.6. 1.7(a)(4); (e) and References</td>
<td>Declassify On</td>
<td>Mandatory</td>
<td>Mandatory, one of: but restricted data or formerly restricted Exemption Category data Event Date and Event</td>
<td>EO 12958: Sec. 1.6, Sec. 2001.21(a)(4), (d), and Subsection 2001.22(d) (references (c) and (au))</td>
</tr>
</tbody>
</table>
C4.1.2. Initial and Current Classification. RMAs shall populate the Current Classification field with the Initial Classification data when the Initial Classification is first entered.

C4.1.3. Current Classification. RMAs shall provide a capability by which a user can edit the Current Classification field prior to filing.

C4.1.4. Originally Classified Records. RMAs shall require that when the "Derived From" field is not completed, the "Classified By" and "Reason(s) for Classification" fields must be completed (see E.O. 12958, part I, section 1.7, reference (c)).

C4.1.5. Derivatively Classified Records. When the "Derived From" field is populated, RMAs shall provide the option of capturing multiple "Reason(s) for Classification" and "Classified By" fields (see 32 CFR 2001.22, reference (au)).

C4.1.6. Derivative Sources. When the classified information is derived from multiple sources, RMAs shall provide the capability to enter multiple sources (see E.O. 12958, Section 2.2 (b) and 32 CFR 2001.22, (references (c) and (au)).

C4.1.7. Declassify On Event. When "Event" is selected in the "Declassify On" field, the RMA shall prompt the user to enter text that describes the declassification event.

C4.1.8. Declassify On Time Frame. When a date is inserted in the "Declassify On" field, RMAs shall verify that the date is no more than the mandated period of time from the Publication Date. If that time frame is exceeded, an alert shall be presented to the user. This mandatory period is currently 10 years (see EO 12958, Section 1.6 (b), reference (c)).

C4.1.9. Maintaining the Declassify On Time Frame. RMAs shall provide the capability for authorized individuals to establish and maintain the period of time used to verify the "Declassify On" field, both to make the retention period more restrictive or to accommodate changes to the mandatory retention period (see EO 12958, Section 1.6 (c) and (d), reference (c)).

C4.1.10. Classification Guides. RMAs shall provide a capability that allows an authorized individual to establish an automatically triggered classification mechanism (see reference (au)). When a designated classification guide indicator is entered in the "Derived From" field, the following fields shall be automatically populated:

- C4.1.10.1. Reason(s) for Classification.
- C4.1.10.2. Initial Classification.
- C4.1.10.3. Declassify On.

C4.1.11. Confirming Accuracy Prior to Filing. RMAs shall provide the capability to confirm the accuracy of all user editable metadata items prior to filing.

C4.1.12. Editing Records. RMAs shall allow only authorized individuals to edit metadata items after a record has been filed.
C4.1.13. Restricted Data and Formerly Restricted Data. The following metadata items are not applicable for records containing Restricted Data or Formerly Restricted Data [Supplemental Marking(s)] and shall be disabled (see EO 12958, Section 6.1 (a), reference (c)).


C4.1.13.2. Declassify On.

C4.1.14. Current Classification. When the entry in the “Current Classification” field is changed, RMAs shall ensure that “Upgraded On,” “Downgraded On,” or “Declassified On” field, whichever is appropriate, is populated with an appropriate date field (see E.O. 12958, Part 3, reference (c)).

C4.1.15. Exemption Categories. RMAs shall provide the capability for an authorized individual to enter or update exemption category(ies) in the “Declassify On” field (see E.O. 12958, Section 3.4 (b) and 32 CFR 2001.21, references (c) and (au)).

C4.1.16. Record History Audit. The RMA shall capture and link an audit history of each record by capturing the replaced metadata value and the person who entered that value, and appending them to a record audit history file. The metadata fields to be captured shall be authorized individual selectable (see E.O. 12958, Part 3 and 32 CFR 2001.21, Subpart E, see references (c) and (au)).

C4.1.17. Using the Record History Audit. The RMA shall provide the capability to view, copy, save, and print the record history file based on user permissions; shall not allow the editing of the record history file; and shall provide the capability for only authorized individuals to delete the record history file.

C4.1.18. Marking Printouts and Displays. Current classification, reasons for classification, and downgrading instructions shall be required metadata items for displays, printouts, reports, queries, review lists, etc. The highest classification level shall be displayed when aggregate results are displayed (see 32 CFR 2001.20, reference (au)).

C4.1.19. The RMA, in conjunction with its operating environment, shall ensure that if there is a conflict between the individual’s access criteria and the access criteria of the group(s) assigned, the individual’s access criteria shall take precedence. (See EO 12958, Part 4; and 32 CFR 2004.4, references (c) and (av)).

C4.1.20. The RMA shall provide a capability whereby authorized individuals restrict access to records and their metadata based on access criteria. In addition to baseline access restriction capabilities, these additional criteria include (see EO 12958, Part 4 and 32 CFR 2004.4, references (c) and (av)).

C4.1.20.1. Current Classification (see subparagraph C4.T1.2.).

C4.1.20.2. Supplemental Marking List (see subparagraph C2.T2.1.6.).

C4.1.20.3. Metadata Elements identified by the organization to be used for access control.

C4.1.21. Access Control. Table C4.T2. summarizes requirements that refer to “authorized individuals” and offers additional information regarding user-type responsibilities. In general, Application Administrators are responsible

---

**Table C4.T2. Authorized Individual Requirements**

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Application Administrator</th>
<th>Records Manager</th>
<th>Privileged User</th>
</tr>
</thead>
<tbody>
<tr>
<td>C4.1.9</td>
<td>Database installed and properly set up</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>to verify the “Declassify On” field, both to make the retention period more restrictive or to accommodate changes to the mandatory retention period.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C4.1.10</td>
<td>Database installed and properly set up</td>
<td>None</td>
<td>Enter and maintain data (Security person)</td>
</tr>
<tr>
<td></td>
<td>Establish an automatically triggered classification mechanism.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C4.1.12</td>
<td>As necessary</td>
<td>As necessary</td>
<td>As necessary (downgrading and reclassification, etc.)</td>
</tr>
<tr>
<td></td>
<td>Edit metadata items after a record has been filed.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C4.1.15</td>
<td>Database installed and properly set up</td>
<td>None</td>
<td>Enter and maintain data (Security person)</td>
</tr>
<tr>
<td></td>
<td>Enter or update exemption category(ies) in the “Declassify On” field.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C4.1.16</td>
<td>As necessary</td>
<td>As necessary</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>Select which metadata field to capture.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C4.1.17</td>
<td>As necessary</td>
<td>As necessary</td>
<td>As necessary</td>
</tr>
<tr>
<td></td>
<td>Delete the record history file.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C4.1.20</td>
<td>User accounts, Access</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>Restrict access to records based on</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
for setting up the RMA infrastructure. Records Managers are responsible for records management administration. Privileged Users are those who are given special permissions to perform functions beyond those of typical users.

C4.2. OPTIONAL SECURITY FEATURES

C4.2.1. RMAs should provide the capability to allow authorized individual-selected metadata fields to be provided their own classification.

C4.2.2. Where appropriate, RMAs should have the capability to inform the user that a redacted version is available in an open RMA.

NOTES

1. Intelligent names are clear, uncoded, identifications of the individual.

2. If accessioning records and metadata to NARA in a format and media specified in 36 CFR 1228.270 causes a violation of the records' authenticity and/or integrity, the organization should contact NARA for guidance, see subparagraph C2.2.10.5.
Electronic Signatures in Global and National Commerce Act
(Public Law 106-229, June 30, 2000)

One Hundred Sixth Congress of the United States of America

AT THE SECOND SESSION

Began and held at the City of Washington on Monday, the twenty-fourth day of January, two thousand

An Act
To facilitate the use of electronic records and signatures in interstate or foreign commerce.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.
This Act may be cited as the ‘Electronic Signatures in Global and National Commerce Act’.

TITLE I—ELECTRONIC RECORDS AND SIGNATURES IN COMMERCE

SEC. 101. GENERAL RULE OF VALIDITY.
(a) IN GENERAL- Notwithstanding any statute, regulation, or other rule of law (other than this title and title II), with respect to any transaction in or affecting interstate or foreign commerce—

(1) a signature, contract, or other record relating to such transaction may not be denied legal effect, validity, or enforceability solely because it is in electronic form; and

(2) a contract relating to such transaction may not be denied legal effect, validity, or enforceability solely because an electronic signature or electronic record was used in its formation.

(b) PRESERVATION OF RIGHTS AND OBLIGATIONS- This title does not—

(1) limit, alter, or otherwise affect any requirement imposed by a statute, regulation, or rule of law relating to the rights and obligations of persons under such statute, regulation, or rule of law other than a requirement that contracts or other records be written, signed, or in nonelectronic form; or

(2) require any person to agree to use or accept electronic records or electronic signatures, other than a governmental agency with respect to a record other than a contract to which it is a party.

(c) CONSUMER DISCLOSURES-

(1) CONSENT TO ELECTRONIC RECORDS- Notwithstanding subsection (a), if a statute, regulation, or other rule of law requires that information relating to a transaction or transactions in or affecting interstate or foreign commerce be provided or made available to a consumer in writing, the use of an electronic record to provide or make available (whichever is required) such information satisfies the requirement that such information be in writing if—

(A) the consumer has affirmatively consented to such use and has not withdrawn such consent;

(B) the consumer, prior to consenting, is provided with a clear and conspicuous statement—

(i) informing the consumer of (I) any right or option of the consumer to have the record provided or made available on paper or in nonelectronic form, and (II) the right of the consumer to withdraw the consent to have the record provided or made available in an electronic form and of any conditions, consequences (which may include termination of the parties’ relationship), or fees in the event of such withdrawal;

(ii) informing the consumer of whether the consent applies (I) only to the particular transaction which gave rise to the obligation to provide the record, or (II) to identified categories of records that may be provided or made available during the course of the parties’ relationship;

(iii) describing the procedures the consumer must use to withdraw consent as provided in clause (i) and to update information needed to contact the consumer electronically; and

(iv) informing the consumer (I) how, after the consent, the consumer may, upon request, obtain a paper copy of an electronic record, and (II) whether any fee will be charged for such copy;

(C) the consumer—

(i) prior to consenting, is provided with a statement of the hardware and software requirements for access to and retention of the electronic records; and

(ii) consents electronically, or confirms his or her consent electronically, in a manner that reasonably demonstrates that the consumer can access information in the electronic form that will be used to provide the information that is the subject of the consent; and

(D) after the consent of a consumer in accordance with subparagraph (A), if a change in the hardware or software requirements needed to access or retain electronic records creates a material risk that the consumer will not be able to access or retain a subsequent electronic record that was the subject of the consent, the person providing the electronic record—

(i) provides the consumer with a statement of (I) the revised hardware and software requirements for access to and retention of the electronic records, and (II) the right to withdraw consent without the imposition of any fees for such withdrawal and without the imposition of any condition or consequence that was not disclosed under subparagraph (B)(i); and

(ii) again complies with subparagraph (C).
(2) OTHER RIGHTS-

(A) PRESERVATION OF CONSUMER PROTECTION- Nothing in this title affects the content or timing of any disclosure or other record required to be provided or made available to any consumer under any statute, regulation, or other rule of law.

(B) VERIFICATION OR ACKNOWLEDGMENT- If a law that was enacted prior to this Act expressly requires a record to be provided or made available by a specified method that requires verification or acknowledgment of receipt, the record may be provided or made available electronically only if the method used provides verification or acknowledgment or receipt (whichever is required).

(3) EFFECT OF FAILURE TO OBTAIN ELECTRONIC CONSENT OR CONFIRMATION OF CONSENT- The legal effectiveness, validity, or enforceability of any contract executed by a consumer shall not be denied solely because of the failure to obtain electronic consent or confirmation of consent by that consumer in accordance with paragraph (1)(C)(ii).

(4) PROSPECTIVE EFFECT- Withdrawal of consent by a consumer shall not affect the legal effectiveness, validity, or enforceability of electronic records provided or made available to that consumer in accordance with paragraph (1) prior to implementation of the consumer’s withdrawal of consent. A consumer’s withdrawal of consent shall be effective within a reasonable period of time after receipt of the withdrawal by the provider of the record.

(5) PRIOR CONSENT- This subsection does not apply to any records that are provided or made available to a consumer who has consented prior to the effective date of this title to receive such records in electronic form as permitted by any statute, regulation, or other rule of law.

(6) ORAL COMMUNICATIONS- An oral communication or a recording of an oral communication shall not qualify as an electronic record for purposes of this subsection except as otherwise provided under applicable law.

(d) RETENTION OF CONTRACTS AND RECORDS-

(1) ACCURACY AND ACCESSIBILITY- If a statute, regulation, or other rule of law requires that a contract or other record relating to a transaction in or affecting interstate or foreign commerce be retained, that requirement is met by retaining an electronic record of the information in the contract or other record that—

(A) accurately reflects the information set forth in the contract or other record; and

(B) remains accessible to all persons who are entitled to access by statute, regulation, or rule of law, for the period required by such statute, regulation, or rule of law, in a form that is capable of being accurately reproduced for later reference, whether by transmission, printing, or otherwise.

(2) EXCEPTION- A requirement to retain a contract or other record in accordance with paragraph (1) does not apply to any information whose sole purpose is to enable the contract or other record to be sent, communicated, or received.

(3) ORIGINALS- If a statute, regulation, or other rule of law requires a contract or other record relating to a transaction in or affecting interstate or foreign commerce to be provided, available, or retained in its original form, or provides consequences if the contract or other record is not provided, available, or retained in its original form, that statute, regulation, or rule of law is satisfied by an electronic record that complies with paragraph (1).

(4) CHECKS- If a statute, regulation, or other rule of law requires the retention of a check, that requirement is satisfied by retention of an electronic record of the information on the front and back of the check in accordance with paragraph (1).

(e) ACCURACY AND ABILITY TO RETAIN CONTRACTS AND OTHER RECORDS- Notwithstanding subsection (a), if a statute, regulation, or other rule of law requires that a contract or other record relating to a transaction in or affecting interstate or foreign commerce be in writing, the legal effect, validity, or enforceability of an electronic record of such contract or other record may be denied if such electronic record is not in a form that is capable of being retained and accurately reproduced for later reference by all parties or persons who are entitled to retain the contract or other record.

(f) PROXIMITY- Nothing in this title affects the proximity required by any statute, regulation, or other rule of law with respect to any warning, notice, disclosure, or other record required to be posted, displayed, or publicly affixed.

(g) NOTARIZATION AND ACKNOWLEDGMENT- If a statute, regulation, or other rule of law requires a signature or record relating to a transaction in or affecting interstate or foreign commerce to be notarized, acknowledged, verified, or made under oath, that requirement is satisfied if the electronic signature of the person authorized to perform those acts, together with all other information required to be included by other applicable statute, regulation, or rule of law, is attached to or logically associated with the signature or record.

(h) ELECTRONIC AGENTS- A contract or other record relating to a transaction in or affecting interstate or foreign commerce may not be denied legal effect, validity, or enforceability solely because its formation, creation, or delivery involved the action of one or more electronic agents so long as the action of any such electronic agent is legally attributable to the person to be bound.

(i) INSURANCE- It is the specific intent of the Congress that this title and title II apply to the business of insurance.

(j) INSURANCE AGENTS AND BROKERS- An insurance agent or broker acting under the direction of a party that enters into a contract by means of an electronic record or electronic signature may not be held liable for any deficiency in the electronic procedures agreed to by the parties under that contract if—
(1) the agent or broker has not engaged in negligent, reckless, or intentional tortious conduct;
(2) the agent or broker was not involved in the development or establishment of such electronic procedures; and
(3) the agent or broker did not deviate from such procedures.

SEC. 102. EXEMPTION TO PREEMPTION.

(a) IN GENERAL.- A State statute, regulation, or other rule of law may modify, limit, or supersede the provisions of section 101 with respect to State law only if such statute, regulation, or rule of law—

(1) constitutes an enactment or adoption of the Uniform Electronic Transactions Act as approved and recommended for enactment in all the States by the National Conference of Commissioners on Uniform State Laws in 1999, except that any exception to the scope of such Act enacted by a State under section 3(b)(4) of such Act shall be preempted to the extent such exception is inconsistent with this title or title II, or would not be permitted under paragraph (2)(A) of this subsection; or

(2)(A) specifies the alternative procedures or requirements for the use or acceptance (or both) of electronic records or electronic signatures to establish the legal effect, validity, or enforceability of contracts or other records, if—

(i) such alternative procedures or requirements are consistent with this title and title II; and

(ii) such alternative procedures or requirements do not require, or accord greater legal status or effect to, the implementation or application of a specific technology or technical specification for performing the functions of creating, storing, generating, receiving, communicating, or authenticating electronic records or electronic signatures; and

(B) if enacted or adopted after the date of enactment of this Act, makes specific reference to this Act.

(b) EXCEPTIONS FOR ACTIONS BY STATES AS MARKET PARTICIPANTS.- Subsection (a)(2)(A)(ii) shall not apply to the statutes, regulations, or other rules of law governing procurement by any State, or any agency or instrumentality thereof.

(c) PREVENTION OF CIRCUMVENTION.- Subsection (a) does not permit a State to circumvent this title or title II through the imposition of nonelectronic delivery methods under section 8(b)(2) of the Uniform Electronic Transactions Act.

SEC. 103. SPECIFIC EXCEPTIONS.

(a) EXCEPTED REQUIREMENTS.- The provisions of section 101 shall not apply to a contract or other record to the extent it is governed by—

(1) a statute, regulation, or other rule of law governing the creation and execution of wills, codicils, or testamentary trusts;

(2) a State statute, regulation, or other rule of law governing adoption, divorce, or other matters of family law; or

(3) the Uniform Commercial Code, as in effect in any State, other than sections 1-107 and 1-206 and Articles 2 and 2A.

(b) ADDITIONAL EXCEPTIONS.- The provisions of section 101 shall not apply to—

(1) court orders or notices, or official court documents (including briefs, pleadings, and other writings) required to be executed in connection with court proceedings;

(2) any notice of—

(A) the cancellation or termination of utility services (including water, heat, and power);

(B) default, acceleration, repossession, foreclosure, or eviction, or the right to cure, under a credit agreement secured by, or a rental agreement for, a primary residence of an individual;

(C) the cancellation or termination of health insurance or benefits or life insurance benefits (excluding annuities); or

(D) recall of a product, or material failure of a product, that risks endangering health or safety; or

(3) any document required to accompany any transportation or handling of hazardous materials, pesticides, or other toxic or dangerous materials.

(c) REVIEW OF EXCEPTIONS.-

(1) EVALUATION REQUIRED.- The Secretary of Commerce, acting through the Assistant Secretary for Communications and Information, shall review the operation of the exceptions in subsections (a) and (b) to evaluate, over a period of 3 years, whether such exceptions continue to be necessary for the protection of consumers. Within 3 years after the date of enactment of this Act, the Assistant Secretary shall submit a report to the Congress on the results of such evaluation.

(2) DETERMINATIONS.- If a Federal regulatory agency, with respect to matters within its jurisdiction, determines after notice and an opportunity for public comment, and publishes a finding, that one or more such exceptions are no longer necessary for the protection of consumers and eliminating such exceptions will not increase the material risk of harm to consumers, such agency may extend the application of section 101 to the exceptions identified in such finding.

SEC. 104. APPLICABILITY TO FEDERAL AND STATE GOVERNMENTS.

(a) FILING AND ACCESS REQUIREMENTS.- Subject to subsection (c)(2), nothing in this title limits or supersedes any requirement by a Federal regulatory agency, self-regulatory organization, or State regulatory agency that records be filed with such agency or organization in accordance with specified standards or formats.
(b) PRESERVATION OF EXISTING RULEMAKING AUTHORITY-

(1) USE OF AUTHORITY TO INTERPRET- Subject to paragraph (2) and subsection (c), a Federal regulatory agency or State regulatory agency that is responsible for rulemaking under any other statute may interpret section 101 with respect to such statute through—

(A) the issuance of regulations pursuant to a statute; or

(B) to the extent such agency is authorized by statute to issue orders or guidance, the issuance of orders or guidance of general applicability that are publicly available and published (in the Federal Register in the case of an order or guidance issued by a Federal regulatory agency). This paragraph does not grant any Federal regulatory agency or State regulatory agency authority to issue regulations, orders, or guidance pursuant to any statute that does not authorize such issuance.

(2) LIMITATIONS ON INTERPRETATION AUTHORITY- Notwithstanding paragraph (1), a Federal regulatory agency shall not adopt any regulation, order, or guidance described in paragraph (1), and a State regulatory agency is preempted by section 101 from adopting any regulation, order, or guidance described in paragraph (1), unless—

(A) such regulation, order, or guidance is consistent with section 101;

(B) such regulation, order, or guidance does not add to the requirements of such section; and

(C) such agency finds, in connection with the issuance of such regulation, order, or guidance, that—

(i) there is a substantial justification for the regulation, order, or guidance;

(ii) the methods selected to carry out that purpose—

(I) are substantially equivalent to the requirements imposed on records that are not electronic records; and

(II) will not impose unreasonable costs on the acceptance and use of electronic records; and

(iii) the methods selected to carry out that purpose do not require, or accord greater legal status or effect to, the implementation or application of a specific technology or technical specification for performing the functions of creating, storing, generating, receiving, communicating, or authenticating electronic records or electronic signatures.

(3) PERFORMANCE STANDARDS-

(A) ACCURACY, RECORD INTEGRITY, ACCESSIBILITY- Notwithstanding paragraph (2)(C)(iii), a Federal regulatory agency or State regulatory agency may interpret section 101(d) to specify performance standards to assure accuracy, record integrity, and accessibility of records that are required to be retained. Such performance standards may be specified in a manner that imposes a requirement in violation of paragraph (2)(C)(iii) if the requirement (i) serves an important governmental objective; and (ii) is substantially related to the achievement of that objective. Nothing in this paragraph shall be construed to grant any Federal regulatory agency or State regulatory agency authority to require use of a particular type of software or hardware in order to comply with section 101(d).

(B) PAPER OR PRINTED FORM- Notwithstanding subsection (c)(1), a Federal regulatory agency or State regulatory agency may interpret section 101(d) to require retention of a record in a tangible printed or paper form if—

(i) there is a compelling governmental interest relating to law enforcement or national security for imposing such requirement; and

(ii) imposing such requirement is essential to attaining such interest.

(4) EXCEPTIONS FOR ACTIONS BY GOVERNMENT AS MARKET PARTICIPANT- Paragraph (2)(C)(iii) shall not apply to the statutes, regulations, or other rules of law governing procurement by the Federal or any State government, or any agency or instrumentality thereof.

(c) ADDITIONAL LIMITATIONS-

(1) REIMPOSING PAPER PROHIBITED- Nothing in subsection (b) (other than paragraph (3)(B) thereof) shall be construed to grant any Federal regulatory agency or State regulatory agency authority to impose or reimpose any requirement that a record be in a tangible printed or paper form.

(2) CONTINUING OBLIGATION UNDER GOVERNMENT PAPERWORK ELIMINATION ACT- Nothing in subsection (a) or (b) relieves any Federal regulatory agency of its obligations under the Government Paperwork Elimination Act (title XVII of Public Law 105-277).

(d) AUTHORITY TO EXEMPT FROM CONSENT PROVISION-

(1) IN GENERAL- A Federal regulatory agency may, with respect to matter within its jurisdiction by regulation or order issued after notice and an opportunity for public comment, exempt without condition a specified category of a record from the requirements relating to consent or type of record from the requirements relating to consent in section 101(c) if such exemption is necessary to eliminate a substantial burden on electronic commerce and will not increase the material risk of harm to consumers.

(2) PROSPECTUSES- Within 30 days after the date of enactment of this Act, the Securities and Exchange Commission shall issue a regulation or order pursuant to paragraph (1) exempting from section 101(c) any records that are required to be provided in order to allow advertising, sales literature, or other information concerning a security issued by an investment company that is registered under the Investment Company Act of 1940, or concerning the issuer thereof, to be excluded from the definition of a prospectus under section 2(a)(10)(A) of the Securities Act of 1933.

(e) ELECTRONIC LETTERS OF AGENCY- The Federal Communications Commission shall not hold any contract for telecommunications service or letter of agency for a pre-
for purposes of this title:

(1) CONSUMER- The term 'consumer' means an individual who obtains, through a transaction, products, or services which are used primarily for personal, family, or household purposes, and also means the legal representative of such an individual.

(2) ELECTRONIC- The term 'electronic' means relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities.

(3) ELECTRONIC AGENT- The term 'electronic agent' means a computer program or an electronic or other automated means used independently to initiate an action or respond to electronic records or performances in whole or in part without review or action by an individual at the time of the action or response.

(4) ELECTRONIC RECORD- The term 'electronic record' means a contract or other record created, generated, sent, communicated, received, or stored by electronic means.

(5) ELECTRONIC SIGNATURE- The term 'electronic signature' means an electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record.

(6) FEDERAL REGULATORY AGENCY- The term 'Federal regulatory agency' means an agency, as that term is defined in section 552(f) of title 5, United States Code.

(7) INFORMATION- The term 'information' means data, text, images, sounds, codes, computer programs, software, databases, or the like.

(8) PERSON- The term 'person' means an individual, corporation, business trust, estate, trust, partnership, limited liability company, association, joint venture, governmental agency, public corporation, or any other legal or commercial entity.

(9) RECORD- The term 'record' means information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form.

(10) REQUIREMENT- The term 'requirement' includes a prohibition.

(11) SELF-REGULATORY ORGANIZATION- The term 'self-regulatory organization' means an organization or entity that is not a Federal regulatory agency or a State, but that is under the supervision of a Federal regulatory agency and is authorized under Federal law to adopt and administer rules applicable to its members that are enforced by such organization or entity, by a Federal regulatory agency, or by another self-regulatory organization.

(12) STATE- The term 'State' includes the District of Columbia and the territories and possessions of the United States.

(13) TRANSACTION- The term 'transaction' means an action or set of actions relating to the conduct of business, consumer, or commercial affairs between two or more persons, including any of the following types of conduct—

(A) the sale, lease, exchange, licensing, or other disposition of (i) personal property, including goods and intangibles, (ii) services, and (iii) any combination thereof; and

(B) the sale, lease, exchange, or other disposition of any interest in real property, or any combination thereof.

SEC. 107. EFFECTIVE DATE.

(a) IN GENERAL- Except as provided in subsection (b), this title shall be effective on October 1, 2000.

(b) EXCEPTIONS-

(1) RECORD RETENTION-

(A) IN GENERAL- Subject to subparagraph (B), this title shall be effective on March 1, 2001, with respect to a requirement that a record be retained imposed by—

(i) a Federal statute, regulation, or other rule of law, or

(ii) a State statute, regulation, or other rule of law administered or promulgated by a State regulatory agency.

(B) DELAYED EFFECT FOR PENDING RULEMAKINGS- If on March 1, 2001, a Federal regulatory agency or State regulatory agency has announced, proposed, or initiated, but not completed, a rulemaking proceeding to
Section 201. Transferable Records.

(a) Definitions- For purposes of this section:

(1) Transferable Record- The term ‘transferable record’ means an electronic record that—
(A) would be a note under Article 3 of the Uniform Commercial Code if the electronic record were in writing;
(B) the issuer of the electronic record expressly has agreed is a transferable record; and
(C) relates to a loan secured by real property.
A transferable record may be executed using an electronic signature.

(2) Other Definitions- The terms ‘electronic record’, ‘electronic signature’, and ‘person’ have the same meanings provided in section 106 of this Act.

(b) Control- A person has control of a transferable record if a system employed for evidencing the transfer of interests in the transferable record reliably establishes that person as the person to which the transferable record was issued or transferred.

(c) Conditions- A system satisfies subsection (b), and a person is deemed to have control of a transferable record, if the transferable record is created, stored, and assigned in such a manner that—

(1) a single authoritative copy of the transferable record exists which is unique, identifiable, and, except as otherwise provided in paragraphs (4), (5), and (6), unalterable; and
(2) the authoritative copy identifies the person asserting control as—

(A) the person to which the transferable record was issued; or
(B) if the authoritative copy indicates that the transferable record has been transferred, the person to which the transferable record was most recently transferred;
(3) the authoritative copy is communicated to and maintained by the person asserting control or its designated custodian;
(4) the person asserting control is the owner of the transferable record;
(5) any revision of the authoritative copy is readily identifiable as authorized or unauthorized.

(d) Status as Holder- Except as otherwise agreed, a person having control of a transferable record is the holder, as defined in section 1-201(20) of the Uniform Commercial Code, of the transferable record and has the same rights and defenses as a holder of an equivalent record or writing under the Uniform Commercial Code, including, if the applicable statutory requirements under section 3-302(a), 9-308, or revised section 9-330 of the Uniform Commercial Code are satisfied, the rights and defenses of a holder in due course or a purchaser, respectively. Delivery, possession, and endorsement are not required to obtain or exercise any of the rights under this subsection.

(e) Obligor Rights- Except as otherwise agreed, an obligor under a transferable record has the same rights and defenses as an equivalent obligor under equivalent records or writings under the Uniform Commercial Code.

(f) Proof of Control- If requested by a person against which enforcement is sought, the person seeking to enforce the transferable record shall provide reasonable proof that the person is in control of the transferable record. Proof may include access to the authoritative copy of the transferable record and related business records sufficient to review the terms of the transferable record and to establish the identity of the person having control of the transferable record.

(g) Ucc References- For purposes of this subsection, all references to the Uniform Commercial Code are to the Uniform Commercial Code as in effect in the jurisdiction the law of which governs the transferable record.

Section 202. Effective Date.

This title shall be effective 90 days after the date of enactment of this Act.

Title III—Promotion of International Electronic Commerce

Section 301. Principles Governing the Use of Electronic Signatures in International Transactions.
(a) PROMOTION OF ELECTRONIC SIGNATURES-

(1) REQUIRED ACTIONS- The Secretary of Commerce shall promote the acceptance and use, on an international basis, of electronic signatures in accordance with the principles specified in paragraph

(2) and in a manner consistent with section 101 of this Act. The Secretary of Commerce shall take all actions necessary in a manner consistent with such principles to eliminate or reduce, to the maximum extent possible, the impediments to commerce in electronic signatures, for the purpose of facilitating the development of interstate and foreign commerce.

(3) PRINCIPLES- The principles specified in this paragraph are the following:


(B) Permit parties to a transaction to determine the appropriate authentication technologies and implementation models for their transactions, with assurance that those technologies and implementation models will be recognized and enforced.

(C) Permit parties to a transaction to have the opportunity to prove in court or other proceedings that their authentication approaches and their transactions are valid.

(D) Take a nondiscriminatory approach to electronic signatures and authentication methods from other jurisdictions.

(b) CONSULTATION- In conducting the activities required by this section, the Secretary shall consult with users and providers of electronic signature products and services and other interested persons.

(c) DEFINITIONS- As used in this section, the terms 'electronic record' and 'electronic signature' have the same meanings provided in section 106 of this Act.

TITLE IV—COMMISSION ON ONLINE CHILD PROTECTION

SEC. 401. AUTHORITY TO ACCEPT GIFTS.

Section 1405 of the Child Online Protection Act (47 U.S.C. 231 note) is amended by inserting after subsection (g) the following new subsection:

(h) GIFTS, BEQUESTS, AND DEVISES- The Commission may accept, use, and dispose of gifts, bequests, or devises of services or property, both real (including the use of office space) and personal, for the purpose of aiding or facilitating the work of the Commission. Gifts or grants not used at the termination of the Commission shall be returned to the donor or grantee.

Speaker of the House of Representatives Vice President of the United States and President of the Senate.

END
Uniform Electronic Transactions Act

SECTION 1. SHORT TITLE.
SECTION 2. DEFINITIONS.
SECTION 3. SCOPE.
SECTION 4. PROSPECTIVE APPLICATION.
SECTION 5. USE OF ELECTRONIC RECORDS AND ELECTRONIC SIGNATURES; VARIATION BY AGREEMENT.
SECTION 6. CONSTRUCTION AND APPLICATION.
SECTION 7. LEGAL RECOGNITION OF ELECTRONIC RECORDS, ELECTRONIC SIGNATURES, AND ELECTRONIC CONTRACTS.
SECTION 8. PROVISION OF INFORMATION IN WRITING; PRESENTATION OF RECORDS.
SECTION 9. ATTRIBUTION AND EFFECT OF ELECTRONIC RECORD AND ELECTRONIC SIGNATURE.
SECTION 10. EFFECT OF CHANGE OR ERROR.
SECTION 11. NOTARIZATION AND ACKNOWLEDGMENT.
SECTION 12. RETENTION OF ELECTRONIC RECORDS; ORIGINALS.
SECTION 13. ADMISSIBILITY IN EVIDENCE.
SECTION 14. AUTOMATED TRANSACTION.
SECTION 15. TIME AND PLACE OF SENDING AND RECEIPT.
SECTION 16. TRANSFERABLE RECORDS.
SECTION 17. CREATION AND RETENTION OF ELECTRONIC RECORDS AND CONVERSION OF WRITTEN RECORDS BY GOVERNMENTAL AGENCIES.
SECTION 18. ACCEPTANCE AND DISTRIBUTION OF ELECTRONIC RECORDS BY GOVERNMENTAL AGENCIES.
SECTION 19. INTEROPERABILITY.
SECTION 20. SEVERABILITY.
SECTION 21. EFFECTIVE DATE.

DRAFT PREFATORY NOTES

With the advent of electronic means of communication and information transfer, business models and methods for doing business have evolved to take advantage of the speed, efficiencies, and cost benefits of electronic technologies. These developments have occurred in the face of existing legal barriers to the legal efficacy of records and documents which exist solely in electronic media. Whether the legal requirement that information or an agreement or contract must be contained or set forth in a pen and paper writing derives from a statute of frauds affecting the enforceability of an agreement, or from a record retention statute that calls for keeping the paper record of a transaction, such legal requirements raise real barriers to the effective use of electronic media.

One striking example of electronic barriers involves so-called check retention statutes in every state. A study conducted by the Federal Reserve Bank of Boston identified more than 2500 different state laws which require the retention of canceled checks by the issuers of those checks. These requirements not only impose burdens on the issuers, but also effectively restrain the ability of banks handling the checks to automate the process. Although check truncation is validated under the Uniform Commercial Code, if the bank’s customer must store the canceled paper check, the bank will not be able to deal with the item through electronic transmission of the information. By establishing the equivalence of an electronic record of the information, the UETA removes these barriers without affecting the underlying legal rules and requirements.

A. Scope of the Act and Procedural Approach. The scope of this Act provides coverage which sets forth a clear framework for covered transactions, and also avoids unwarranted surprises for unsophisticated parties dealing in this relatively new media. The clarity and certainty of the scope of the Act have been obtained while still providing a solid legal framework that allows for the continued development of innovative technology to facilitate electronic transactions.

With regard to the general scope of the Act, the Act’s coverage is inherently limited by the definition of “transaction.” The Act does not apply to all writings and signatures, but only to electronic records and signatures relating to a transaction, defined as those interactions between people relating to business, commercial and governmental affairs. In general, there are few writing or signature requirements imposed by law on many of the “standard” transactions that had been considered for exclusion. A good example relates to trusts, where the general rule on creation of a trust imposes no formal writing requirement. Further, the writing requirements in other contexts derived from governmental filing issues. For example, real estate transactions were considered potentially troublesome because of the need to file a deed or other instrument for protection against third parties. Since the efficacy of a real estate purchase contract, or even a deed, between the parties is not affected by any sort of filing, the question was raised why these transactions should not be validated by this Act if done via an electronic medium. No sound reason was found. Filing requirements fall within Sections 17-19 on governmental records. An exclusion of all real estate transactions would be particularly unwarranted in the event that a state chose to convert to an electronic recording system, as many have for Article 9 financing statement filings under the Uniform Commercial Code.

The exclusion of specific Articles of the Uniform Commercial Code reflects the recognition that, particularly in the case of Articles 5, 8 and revised Article 9, electronic transactions were addressed in the specific contexts of those revision processes. In the context of Articles 2 and 2A the UETA provides the vehicle for assuring that such transactions may be accomplished and effected via
an electronic medium. At such time as Articles 2 and 2A are revised the extent of coverage in those Articles/Acts may make application of this Act as a gap-filling law desirable. Similar considerations apply to the recently promulgated Uniform Computer Information Transactions Act (“UCITA”).

The need for certainty as to the scope and applicability of this Act is critical, and makes any sort of a broad, general exception based on notions of inconsistency with existing writing and signature requirements unwise at best. The uncertainty inherent in leaving the applicability of the Act to judicial construction of this Act with other laws is unacceptable if electronic transactions are to be facilitated.

Finally, recognition that the paradigm for the Act involves two willing parties conducting a transaction electronically, makes it necessary to expressly provide that some form of acquiescence or intent on the part of a person to conduct transactions electronically is necessary before the Act can be invoked. Accordingly, Section 5 specifically provides that the Act only applies between parties that have agreed to conduct transactions electronically. In this context, the construction of the term agreement must be broad in order to assure that the Act applies whenever the circumstances show the parties intention to transact electronically, regardless of whether the intent rises to the level of a formal agreement.

B. Procedural Approach. Another fundamental premise of the Act is that it be minimalist and procedural. The general efficacy of existing law, in an electronic context, so long as biases and barriers to the medium are removed, confirms this approach. The Act defers to existing substantive law. Specific areas of deference to other law in this Act include: 1) the meaning and effect of “sign” under existing law, 2) the method and manner of displaying, transmitting and formatting information in section 8, 3) rules of attribution in section 9, and 4) the law of mistake in section 10.

The Act’s treatment of records and signatures demonstrates best the minimalist approach that has been adopted. Whether a record is attributed to a person is left to law outside this Act. Whether an electronic signature has any effect is left to the surrounding circumstances and other law. These provisions are salutary directives to assure that records and signatures will be treated in the same manner, under currently existing law, as written records and manual signatures.

The deference of the Act to other substantive law does not negate the necessity of setting forth rules and standards for using electronic media. The Act expressly validates electronic records, signatures and contracts. It provides for the use of electronic records and information for retention purposes, providing certainty in an area with great potential in cost savings and efficiency. The Act makes clear that the actions of machines (“electronic agents”) programmed and used by people will bind the user of the machine, regardless of whether human review of a particular transaction has occurred. It specifies the standards for sending and receipt of electronic records, and it allows for innovation in financial services through the implementation of transferable records. In these ways the Act permits electronic transactions to be accomplished with certainty under existing substantive rules of law.

UNIFORM ELECTRONIC TRANSACTIONS ACT

SECTION 1. SHORT TITLE. This [Act] may be cited as the Uniform Electronic Transactions Act.

SECTION 2. DEFINITIONS. In this [Act]:

(1) “Agreement” means the bargain of the parties in fact, as found in their language or inferred from other circumstances and from rules, regulations, and procedures given the effect of agreements under laws otherwise applicable to a particular transaction.

(2) “Automated transaction” means a transaction conducted or performed, in whole or in part, by electronic means or electronic records, in which the acts or records of one or both parties are not reviewed by an individual in the ordinary course in forming a contract, performing under an existing contract, or fulfilling an obligation required by the transaction.

(3) “Computer program” means a set of statements or instructions to be used directly or indirectly in an information processing system in order to bring about a certain result.

(4) “Contract” means the total legal obligation resulting from the parties’ agreement as affected by this [Act] and other applicable law.

(5) “Electronic” means relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities.

(6) “Electronic agent” means a computer program or an electronic or other automated means used independently to initiate an action or respond to electronic records or performances in whole or in part, without review or action by an individual.

(7) “Electronic record” means a record created, generated, sent, communicated, received, or stored by electronic means.

(8) “Electronic signature” means an electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record.

(9) “Governmental agency” means an executive, legislative, or judicial agency, department, board, commission, authority, institution, or instrumentality of the federal government or of a State or of a county, municipality, or other political subdivision of a State.

(10) “Information” means data, text, images, sounds, codes, computer programs, software, databases, or the like.

(11) “Information processing system” means an electronic system for creating, generating, sending, receiving, storing, displaying, or processing information.

(12) “Person” means an individual, corporation, business trust, estate, trust, partnership, limited liability company,
association, joint venture, governmental agency, public corporation, or any other legal or commercial entity.

(13) “Record” means information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form.

(14) “Security procedure” means a procedure employed for the purpose of verifying that an electronic signature, record, or performance is that of a specific person or for detecting changes or errors in the information in an electronic record. The term includes a procedure that requires the use of algorithms or other codes, identifying words or numbers, encryption, or callback or other acknowledgment procedures.

(15) “State” means a State of the United States, the District of Columbia, Puerto Rico, the United States Virgin Islands, or any territory or insular possession subject to the jurisdiction of the United States. The term includes an Indian tribe or band, or Alaskan native village, which is recognized by federal law or formally acknowledged by a State.

(16) “Transaction” means an action or set of actions occurring between two or more persons relating to the conduct of business, commercial, or governmental affairs.

Sources: UNICTRAL Model Law on Electronic Commerce; Uniform Commercial Code; Uniform Computer Information Transactions Act; Restatement 2d Contracts.

DRAFT COMMENTS

1. “Agreement.” Whether the parties have reached an agreement is determined by their express language and all surrounding circumstances. The Restatement of Contracts 2d §3 provides that, “An agreement is a manifestation of mutual assent on the part of two or more persons.” See also Restatement of Contracts 2d, Section 2, Comment b. The Uniform Commercial Code specifically includes in the circumstances from which an agreement may be inferred “course of performance, course of dealing and usage of trade...” as defined in the UCC. Although the definition of agreement in this Act does not make specific reference to usage of trade and other party conduct, this definition is not intended to affect the construction of the parties’ agreement under the substantive law applicable to a particular transaction. Where that law takes account of usage and conduct in informing the terms of the parties’ agreement, the usage or conduct would be relevant as “other circumstances” included in the definition under this Act.

Where the law applicable to a given transaction provides that system rules and the like constitute part of the agreement of the parties, such rules will have the same effect in determining the parties agreement under this Act. For example, UCC Article 4 (Section 4-103(b)) provides that Federal Reserve regulations and operating circulars and clearinghouse rules have the effect of agreements. Such agreements by law properly would be included in the definition of agreement in this Act.

The parties’ agreement is relevant in determining whether the provisions of this Act have been varied by agreement.

In addition, the parties’ agreement may establish the parameters of the parties’ use of electronic records and signatures, security procedures and similar aspects of the transaction. See Model Trading Partner Agreement, 45 Business Lawyer Supp. Issue (June 1990). See Section 5(b) and comments thereto.

2. “Automated Transaction.” This definition addresses the use and effectiveness of machines beyond the issue of contract formation and deals with performances under a contract and other obligations accomplished by electronic means in a transaction. Such a broad application is necessary because of the diversity of transactions to which this Act may apply.

As with electronic agents, this definition addresses the circumstance where electronic records may result in action or performance by a party although no human review of the electronic records is anticipated. Section 14 provides specific rules to assure that where one or both parties do not review the electronic records, the resulting agreement will be effective.

The critical element in this definition is the lack of a human actor on one or both sides of a transaction. For example, if one orders books from Bookseller.com through Bookseller’s website, the transaction would be an automated transaction because Bookseller took and confirmed the order via its machine. Similarly, if Automaker and supplier do business through Electronic Data Interchange, Automaker’s computer, upon receiving information within certain pre-programmed parameters, will send an electronic order to supplier’s computer. If Supplier’s computer confirms the order and processes the shipment because the order falls within pre-programmed parameters in Supplier’s computer, this would be a fully automated transaction. If, instead, the Supplier relies on a human employee to review, accept, and process the Buyer’s order, then only the Automaker’s side of the transaction would be automated. In either case, the entire transaction falls within this definition.

3. “Computer program.” This definition refers to the functional and operating aspects of an electronic, digital system. It relates to operating instructions used in an electronic system such as an electronic agent. (See definition of “Electronic Agent.”)

4. “Electronic.” The basic nature of most current technologies and the need for a recognized, single term warrants the use of “electronic” as the defined term. The definition is intended to assure that the Act will be applied broadly as new technologies develop. The term must be construed broadly in light of developing technologies in order to fulfill the purpose of this Act to validate commercial transactions regardless of the medium used by the parties. Current legal requirements for “writings” can be satisfied by most any tangible media, whether paper, other fibers, or even stone. The purpose and applicability of this Act covers intangible media which are technologically capable of storing, transmitting and reproducing...
information in human perceivable form, but which lack the tangible aspect of paper, papyrus or stone.

While not all technologies listed are technically “electronic” in nature (e.g., optical fiber technology), the term “electronic” is the most descriptive term available to describe the majority of current technologies. For example, the development of biological and chemical processes for communication and storage of data, while not specifically mentioned in the definition, are included within the technical definition because such processes operate on electromagnetic impulses. However, whether a particular technology may be characterized as technically “electronic,” i.e., operates on electromagnetic impulses, should not be determinative of whether records and signatures created, used and stored by means of a particular technology are covered by this Act. This act is intended to apply to all records and signatures created, used and stored by any medium which permits the information to be retrieved in perceivable form.

5. **“Electronic agent.”** This definition establishes that an electronic agent is a machine. As the term “electronic agent” has come to be recognized, it is limited to a tool function. The effect on the party using the agent is addressed in the operative provisions of the Act (e.g., Section 14).

An electronic agent, such as a computer program or other automated means employed by a person, is a tool of that person. As a general rule, the employer of a tool is responsible for the results obtained by the use of that tool since the tool has no independent volition of its own. However, an electronic agent, by definition, is capable within the parameters of its programming, of initiating, responding or interacting with other parties or their electronic agents once it has been activated by a party, without further attention of that party.

While this Act proceeds on the paradigm that an electronic agent is capable of performing only within the technical strictures of its preset programming, it is conceivable that, within the useful life of this Act, electronic agents may be created with the ability to act autonomously, and not just automatically. That is, through developments in artificial intelligence, a computer may be able to “learn through experience, modify the instructions in their own programs, and even devise new instructions.” Allen and Widdison, “Can Computers Make Contracts?” 9 Harv. J.L.&Tech 25 (Winter, 1996). If such developments occur, courts may construe the definition of electronic agent accordingly, in order to recognize such new capabilities.

The examples involving Bookseller.com and Automaker in the comment to the definition of Automated Transaction are equally applicable here. Bookseller acts through an electronic agent in processing an order for books. Automaker and the supplier each act through electronic agents in facilitating and effectuating the just-in-time inventory process through EDI.

6. **“Electronic record.”** An electronic record is a subset of the broader defined term “record.” It is any record created, used or stored in a medium other than paper (see definition of electronic). The defined term is also used in this Act as a limiting definition in those provisions in which it is used.

Information processing systems, computer equipment and programs, electronic data interchange, electronic mail, voice mail, facsimile, telex, telecopying, scanning, and similar technologies all qualify as electronic under this act. Accordingly information stored on a computer hard drive or floppy disc, facsimiles, voice mail messages, messages on a telephone answering machine, audio and video tape recordings, among other records, all would be electronic records under this Act.

7. **“Electronic signature.”** The idea of a signature is broad and not specifically defined. Whether any particular record is “signed” is a question of fact. Proof of that fact must be made under other applicable law. This act simply assures that the signature may be accomplished through an electronic means. No specific technology need be used in order to create a valid signature. One’s voice on an answering machine may suffice if the requisite intention is present. Similarly, including one’s name as part of an electronic mail communication also may suffice, as may the firm name on a facsimile. It also may be shown that the requisite intent was not present and accordingly the symbol, sound or process did not amount to a signature. One may use a digital signature with the requisite intention, or one may use the private key solely as an access device with no intention to sign, or otherwise accomplish a legally binding act. In any case the critical element is the intention to execute or adopt the sound or symbol or process for the purpose of signing the related record.

The definition requires that the signer execute or adopt the sound, symbol, or process with the intent to sign the record. The act of applying a sound, symbol or process to an electronic record could have differing meanings and effects. The consequence of the act and the effect of the act as a signature are determined under other applicable law. However, the essential attribute of a signature involves applying a sound, symbol or process with an intent to do a legally significant act. It is that intention that is understood in the law as a part of the word “sign,” without the need for a definition.

This Act establishes, to the greatest extent possible, the equivalency of electronic signatures and manual signatures. The purpose is to overcome unwarranted biases against electronic means of signing and authenticating records. Therefore the term “signature” has been used to connote and convey that equivalency. The term “authentication,” used in other laws, often has a narrower meaning and purpose than an electronic signature as used in this Act. However, an authentication under any of those other laws constitutes an electronic signature under this Act.
The precise effect of an electronic signature will be determined based on the surrounding circumstances under section 9(b).

This definition includes as an electronic signature the standard webpage click-through process. For example, when a person orders goods or services through a vendor’s website, the person will be required to provide information as part of a process which will result in receipt of the goods or services. When the customer ultimately gets to the last step and clicks “I agree,” the person has adopted the process and has done so with the intent to associate the person with the record of that process. The actual effect of the electronic signature will be determined from all the surrounding circumstances, however, the person adopted a process which the circumstances indicate s/he intended to have the effect of getting the goods/services and being bound to pay for them. The adoption of the process carried the intent to do a legally significant act, the hallmark of a signature.

Another important aspect of this definition lies in the necessity that the electronic signature be linked or logically associated with the record. In the paper world, it is assumed that the symbol adopted by a party is attached to or located somewhere in the same paper that is intended to be authenticated, e.g., an allonge firmly attached to a promissory note, or the classic signature at the end of a long contract. These tangible manifestations do not exist in the electronic environment, and accordingly, this definition expressly provides that the symbol must in some way be linked to, or connected with, the electronic record being signed. This linkage is consistent with the regulations promulgated by the Food and Drug Administration, 21 CFR Part 11 (March 20, 1997).

A digital signature using public key encryption technology would qualify as an electronic signature, as would the mere inclusion of one’s name as a part of an e-mail message - so long as in each case the signer executed or adopted the symbol with the intent to sign.

8. “Governmental agency.” This definition is important in the context of optional Sections 17-19.

9. “Information processing system.” This definition is consistent with the UNCITRAL Model Law on Electronic Commerce. The term includes computers and other information systems. It is principally used in Section 15 in connection with the sending and receiving of information. In that context, the key aspect is that the information enter a system from which a person can access it.

10. “Record.” This is a standard definition designed to embrace all means of communicating or storing information except human memory. It includes any method for storing or communicating information, including “writings.” A record need not be indestructible or permanent, but the term does not include oral or other communications which are not stored or preserved by some means. Information that has not been retained other than through human memory does not qualify as a record. As in the case of the terms “writing” or “written,” the term “record” does not establish the purposes, permitted uses or legal effect which a record may have under any particular provision of substantive law. ABA Report on Use of the Term “Record,” October 1, 1996.

11. “Security procedure.” A security procedure may be applied to verify an electronic signature, verify the identity of the sender, or assure the informational integrity of an electronic record. The definition does not identify any particular technology. This permits the use of procedures which the parties select or which are established by law. It permits the greatest flexibility among the parties and allows for future technological development.

The definition in this Act is broad and is used to illustrate one way of establishing attribution or content integrity of an electronic record or signature. The use of a security procedure is not accorded operative legal effect, through the use of presumptions or otherwise, by this Act. In this Act, the use of security procedures is simply one method for proving the source or content of an electronic record or signature.

A security procedure may be technologically very sophisticated, such as an asymmetric cryptographic system. At the other extreme the security procedure may be as simple as a telephone call to confirm the identity of the sender through another channel of communication. It may include the use of a mother’s maiden name or a personal identification number (PIN). Each of these examples is a method for confirming the identity of a person or accuracy of a message.

12. “Transaction.” The definition has been limited to actions between people taken in the context of business, commercial or governmental activities. The term includes all interactions between people for business, commercial, including specifically consumer, or governmental purposes. However, the term does not include unilateral or nontransactional actions. As such it provides a structural limitation on the Scope of the Act as stated in the next section.

It is essential that the term commerce and business be understood and construed broadly to include commercial and business transactions involving individuals who may qualify as “consumers” under other applicable law. If Alice and Bob agree to the sale of Alice’s car to Bob for $2000 using an Internet auction site, that transaction is fully covered by this Act. Even if Alice and Bob each qualify as typical “consumers,” under other applicable law, their interaction was a transaction in commerce. Accordingly their actions would be related to commercial affairs, and fully qualify as a transaction governed by this Act.

Other transaction types may include:

1. A single purchase by an individual from a retail merchant, which may be accomplished by an order sent by facsimile from a printed catalog, or by exchange of electronic mail;
2. Recurring orders on a weekly or monthly basis between large companies which have entered into a master trading
partner agreement to govern the methods and manner of their transaction parameters;

3. A purchase by an individual from an online Internet retail vendor. Such an arrangement may develop into an ongoing series of individual purchases, with security procedures and the like, as a part of doing ongoing business.

4. The closing of a business purchase transaction via facsimile transmission of documents or electronic mail. In such a transaction, all parties may participate through electronic conferencing technologies. At the appointed time all electronic records are executed electronically and transmitted to the other party. In such a case, the electronic records and electronic signatures are validated under this Act, obviating the need for “in person” closings.

A transaction must include interaction between two or more persons. Accordingly, the execution of a will or trust, or the execution of a health care power of attorney or similar health care designation, for example, would not be covered by this Act because they are not a part of a transaction as defined in this Act.

SECTION 3. SCOPE.

(a) Except as otherwise provided in subsection (b), this [Act] applies to electronic records and electronic signatures relating to a transaction.

(b) This [Act] does not apply to a transaction to the extent it is governed by:

(1) a law governing the creation and execution of wills, codicils, or testamentary trusts;

(2) [The Uniform Commercial Code other than Sections 1-107 and 1-206, Article 2, and Article 2A];

(3) [the Uniform Computer Information Transactions Act]; and

(4) [other laws, if any, identified by State].

(c) This [Act] applies to an electronic record or electronic signature otherwise excluded from the application of this [Act] under subsection (b) to the extent it is governed by a law other than those specified in subsection (b).

(d) A transaction subject to this [Act] is also subject to other applicable substantive law.

SEE LEGISLATIVE NOTE BELOW – FOLLOWING DRAFT COMMENTS.

DRAFT COMMENTS

1. The Scope of this Act is inherently limited by the fact that it only applies to transactions related to business, commercial (including consumer) and governmental matters. Consequently, transactions with no relation to business, commercial or governmental transactions would not be subject to this Act. Unilaterally generated electronic records and signatures which are not part of a transaction also are not covered by this Act. See Section 2, Comment 12.

2. This act affects the medium in which information, records and signatures may be presented and retained under current legal requirements. While this Act covers all electronic records and signatures which are used in a business, commercial (including consumer) or governmental transaction, the operative provisions of the act relate to requirements for writings and signatures under other laws. Accordingly, the exclusions in subsection (b) focus on those legal rules imposing certain writing and signature requirements which will not be affected by this Act.

3. The exclusions listed in subsection (b) provide clarity and certainty regarding the laws which are and are not affected by this Act. This section provides that transactions subject to specific laws are unaffected by this Act and leaves the balance subject to this Act.

4. Paragraph (1) excludes wills, codicils and testamentary trusts. This exclusion is largely salutary given the unilateral context in which such records are generally created and the unlikely use of such records in a transaction as defined in this Act (i.e., actions taken by two or more persons in the context of business, commercial or governmental affairs).

5. Articles 3, 4 and 4A of the UCC impact payment systems and have specifically been removed from the coverage of this Act. Moreover, the systems affected go well beyond the relationships between contracting parties and require broader attention to systemic effects. Articles 5, 8 and 9 have been excluded because the revision process relating to those Articles included significant consideration of electronic practices. Paragraph 4 provides for exclusion from this Act of UCITA because the drafting process of that Act also included significant consideration of electronic contracting provisions.

6. The very limited application of this Act to Transferable Records in Section 16 does not affect payment systems, and the Section is designed to apply to a transaction through express agreement of the parties. The exclusion of Articles 3 and 4 will not affect the Act’s coverage of Transferable Records. Section 16 is designed to allow for the development of systems which will provide “control” as defined in Section 16. Such control is necessary as a substitute for the idea of possession which undergirds negotiable instrument law. The technology has yet to be developed which will allow for the possession of a unique electronic token embodying the rights associated with a negotiable promissory note. Section 16’s concept of control is intended as a substitute for possession.

The provisions in Section 16 operate as free standing rules, establishing the rights of parties using Transferable Records under this Act. The references in Section 16 to UCC Section 3-302, 7-501 and 9-308 (R9-330(d)) are designed to incorporate the substance of those provisions into this act for the limited purposes noted in section 16(c). Accordingly, an electronic record which is also a Transferable Record, would not be used for purposes of a transaction governed by Articles 3, 4, or 9, but would be
an electronic record used for purposes of a transaction governed by Section 16. However, it is important to remember that those UCC Articles will still apply to the transferable record in their own right. Accordingly any other substantive requirements, e.g., method and manner of perfection under Article 9, must be complied with under those other laws. See Comments to Section 16.

7. This Act does apply, in toto, to transactions under unrevised Articles 2 and 2A. There is every reason to validate electronic contracting in these situations. Sales and leases do not implicate broad systems such as is the case with payment systems. Further sales and leases generally do not have a far reaching effect on the rights of parties beyond the contracting parties, such as exists in the secured transactions system. Finally, it is in the area of sales, licenses and leases that electronic commerce is occurring to its greatest extent today. To exclude these transactions would largely gut the purpose of this Act.

In the event that Articles 2 and 2A are revised and adopted in the future, UETA will only apply to the extent provided in those Acts.

8. An electronic record/signature may be used for purposes of more than one legal requirement, or may be covered by more than one law. Consequently, it is important to make clear, despite any apparent redundancy, in subsection (c) that an electronic record used for purposes of a law which is not affected by this act under subsection (b) may nonetheless be used and validated for purposes of other laws not excluded by subsection (b). For example, this Act does not apply to an electronic record of a check when used for purposes of a transaction governed by Article 4 of the Uniform Commercial Code, i.e., the Act does not validate so-called electronic checks.

Because of the overwhelming number of references in state law to writings and signatures, the following list of possible transactions would largely gut the purpose of this Act. To exclude these transactions would largely gut the purpose of this Act. In the event that Articles 2 and 2A are revised and adopted in the future, UETA will only apply to the extent provided in those Acts.

9. Additional exclusions under subparagraph (b)(4) should be limited to laws which govern electronic records and signatures which may be used in transactions as defined in Section 2(16). Records used unilaterally, or which do not relate to business, commercial (including consumer), or governmental affairs are not governed by this Act in any event, and exclusion of laws relating to such records may create unintended inferences about whether other records and signatures are covered by this Act.

It is also important that additional exclusions, if any, be included under subsection (b)(4) in order to assure that continued validation of such records under subsection (c) will occur.

LEGISLATIVE NOTE REGARDING POSSIBLE ADDITIONAL EXCLUSIONS UNDER SECTION 3(b)(4).

The following discussion is derived from the Report dated September 21, 1998 of The Task Force on State Law Exclusions (the “Task Force”) presented to the Drafting Committee. After consideration of the Report, the Drafting Committee determined that exclusions other than those specified in the Act were not warranted. In addition, other inherent limitations on the applicability of the act (the definition of transaction, the requirement that the parties acquiesce in the use of an electronic format) also militate against additional exclusions. Nonetheless, the Drafting Committee recognized that some legislatures may wish to exclude additional transactions from the act, and determined that guidance in some major areas would be helpful to those legislatures considering additional areas for exclusion.

Because of the overwhelming number of references in state law to writings and signatures, the following list of possible transactions is not exhaustive. However, they do represent those areas most commonly raised during the course of the drafting process as areas that might be inappropriate for an electronic medium. It is important to keep in mind however, that the drafting committee determined that exclusion of these additional areas was not warranted.

1. Trusts (other than testamentary trusts). Trusts can be used for both business and personal purposes. By virtue of the definition of transaction, trusts used outside the area of business and commerce would not be governed by this Act. With respect to business or commercial trusts, the laws governing their formation contain few or no requirements for paper or signatures. Indeed, in most jurisdictions trusts of any kind may be created orally. Consequently, the drafting committee believed that the Act should apply to any transaction where the law leaves to the parties the decision of whether to use a writing. Thus, in the absence of legal requirements for writings, there is no sound reason to exclude laws governing trusts from the application of this Act.

2. Powers of Attorney. A power of attorney is simply a formalized type of agency agreement. In general, no formal requirements for paper or execution were found to be applicable to the validity of powers of attorney.

Special health powers of attorney have been established by statute in some states. These powers may have special requirements under state law regarding execution, acknowledgment and possibly notarization. In the normal case such powers will not arise in a transactional context and so would not be covered by this Act. However, even if such a record were to arise in a transactional context, this act operates simply to remove the barrier to the
use of an electronic medium, and preserves other requirements of applicable substantive law, avoiding any necessity to exclude such laws from the operation of this Act. Especially in light of the provisions of Sections 8 and 11, the substantive requirements under such laws will be preserved and may be satisfied in an electronic format.

3. Real Estate Transactions. It is important to distinguish between the efficacy of paper documents involving real estate between the parties, as opposed to their effect on third parties. The latter consideration relates to the necessity of governmental filing. As between the parties, it is unnecessary to maintain existing barriers to electronic contracting. There are no unique characteristics to contracts relating to real property as opposed to other business and commercial (including consumer) contracts. Consequently, the decision whether to use an electronic medium for their agreements should be a matter for the parties to determine. In the event notarization and acknowledgment are required under other laws, Section 11 provides a means for such actions to be accomplished electronically.

With respect to the requirements of government filing, those are left to the individual states in the decision of whether to adopt and implement electronic filing systems. (See optional Section 17-19). However, government recording systems currently require paper deeds including notarized, manual signatures. Although California and Illinois are experimenting with electronic filing systems, until such systems become widespread, the parties likely will choose to use, at the least, a paper deed for filing purposes. Nothing in this Act precludes the parties from selecting the medium best suited to the needs of the particular transaction. Parties may wish to consummate the transaction using electronic media in order to avoid expensive travel. Yet the actual deed may be in paper form to assure compliance with existing recording systems and requirements. The critical point is that nothing in this Act prevents the parties from selecting paper or electronic media for all or part of their transaction.

4. Consumer Protection Statutes. Consumer protection provisions in state law often require that information be disclosed or provided to a consumer in writing. Because this act does apply to such transactions, the question of whether such laws should be specifically excluded was considered. Exclusion of consumer transactions would eliminate a huge group of commercial transactions which benefit consumers by enabling the efficiency of the electronic medium. Commerce over the Internet is driven by consumer demands and concerns and must be included.

At the same time, it is important to recognize the protective effects of many consumer statutes. Consumer statutes often require that information be provided in writing, or may require that the consumer separately sign or initial a particular provision to evidence that the consumer’s attention was brought to the provision. Subsection (1) requires electronic records to be retainable by a person whenever the law requires information to be delivered in writing. The section imposes a significant burden on the sender of information. The sender must be assured that the information system of the recipient is compatible with, and capable of retaining the information sent by, the sender’s system. Furthermore, nothing in this Act permits the avoidance of legal requirements of separate signatures or initialing. The Act simply permits the signature or initialing to be done electronically.

Other consumer protection statutes require (expressly or implicitly) that certain information be presented in a certain manner or format. Laws requiring information to be presented in particular fonts, formats or in similar fashion, as well as laws requiring conspicuous displays of information are preserved. Section 8(b)(3) specifically preserves the applicability of such requirements in an electronic environment. In the case of conspicuous requirements, the determination of what is conspicuous will be left to other law. Section 8 was included to specifically preserve the protective functions of such disclosure statutes, while at the same time allowing the use of electronic media if the substantive requirements of the other laws could be satisfied in the electronic medium.

The requirement that both parties agree to conduct a transaction electronically also prevents the imposition of the electronic medium on unwilling parties. See Section 5(b). In addition, where the law requires inclusion of specific terms or language, those requirements are preserved broadly by Section 5(e).

Requirements that information be sent to, or received by, someone have been preserved in Section 15. As in the paper world, obligations to send do not impose any duties on the sender to assure receipt, other than reasonable methods of dispatch. In those cases where receipt is required legally, Sections 5, 8 and 15 impose the burden on the sender to assure delivery to the recipient if satisfaction of the legal requirement is to be fulfilled.

Formatting and separate signing requirements serve a critical purpose in much consumer protection legislation, to assure that information is not slipped past the unsuspecting consumer. Not only does this Act not disturb those requirements, it preserves those requirements. In addition, other bodies of substantive law continue to operate to allow the courts to police any such bad conduct or overreaching, e.g., unconscionability, fraud, duress, mistake and the like. These bodies of law remain applicable regardless of the medium in which a record appears.

The preservation of existing safeguards, together with the ability to opt out of the electronic medium entirely, demonstrate the lack of any need generally to exclude consumer protection laws from the operation of this Act. Legislatures may wish to focus any review on those statutes which provide for post-contract formation and post-breach notices to be in paper. However, any such consideration must also balance the needed protections against the potential burdens which may be imposed. Consumers and others will not be well served by restrictions which preclude the employment of electronic technologies sought and desired by consumers.
SECTION 4. PROSPECTIVE APPLICATION. This Act applies to any electronic record or electronic signature created, generated, sent, communicated, received, or stored on or after the effective date of this Act.

DRAFT COMMENT
This section makes clear that the Act only applies to validate electronic records and signatures arising after the effective date of the Act. Whether electronic records and electronic signatures arising before the effective date of this Act are valid is left to other law.

SECTION 5. USE OF ELECTRONIC RECORDS AND ELECTRONIC SIGNATURES; VARIATION BY AGREEMENT.
(a) This Act does not require a record or signature to be created, generated, sent, communicated, received, stored, or otherwise processed or used by electronic means or in electronic form.
(b) This Act applies only to transactions between parties each of which has agreed to conduct transactions by electronic means. Whether the parties agree to conduct a transaction by electronic means is determined from the context and surrounding circumstances, including the parties’ conduct.
(c) A party that agrees to conduct a transaction by electronic means may refuse to conduct other transactions by electronic means. The right granted by this subsection may not be waived by agreement.
(d) Except as otherwise provided in this Act, the effect of any of its provisions may be varied by agreement. The presence in certain provisions of this Act of the words “unless otherwise agreed”, or words of similar import, does not imply that the effect of other provisions may not be varied by agreement.
(e) Whether an electronic record or electronic signature has legal consequences is determined by this Act and other applicable law.

DRAFT COMMENTS
This Section limits the applicability of this Act to transactions which parties have agreed to conduct electronically. Accordingly, a broad interpretation of the term agreement is necessary to assure that this Act has the widest possible application consistent with its purpose of removing barriers to electronic commerce.
1. This section makes clear that this Act is intended to facilitate the use of electronic means, but does not require the use of electronic records and signatures. This fundamental principle is set forth in subsection (a) and elaborated by subsections (b) and (c), which require an intention to conduct transactions electronically and preserve the right of a party to refuse to use electronics in any subsequent transaction.
2. The paradigm of this Act is two willing parties doing transactions electronically. It is therefore appropriate that the Act is voluntary and preserves the greatest possible party autonomy to refuse electronic transactions. The requirement that party agreement be found from all the surrounding circumstances is a limitation on the scope of this Act.
3. If this Act is to serve to facilitate electronic transactions, it must be applicable under circumstances not rising to a full fledged contract to use electronics. While absolute certainty can be accomplished by obtaining an explicit contract before relying on electronic transactions, such an explicit contract should not be necessary before one may feel safe in conducting transactions electronically. Indeed, such a requirement would itself be an unreasonable barrier to electronic commerce, at odds with the fundamental purpose of this Act. Accordingly, the requisite agreement, express or implied, must be determined from all available circumstances and evidence.
4. Subsection (b) provides that the Act applies to transactions in which the parties have agreed to conduct the transaction electronically. In this context it is essential that the parties’ actions and words be broadly construed in determining whether the requisite agreement exists. Accordingly, the Act expressly provides that the party’s agreement is to be found from all circumstances, including the parties’ conduct. The critical element is the intent of a party to conduct a transaction electronically. Once that intent is established, this Act applies. See Restatement of Contracts 2d, Sections 2, 3 and 19.

Examples of circumstances from which it may be found that parties have reached an agreement to conduct transactions electronically include the following:
EXAMPLES:
A. Automaker and supplier enter into a Trading Partner Agreement setting forth the terms, conditions and methods for the conduct of business between them electronically.
B. Joe gives out his business card with his business e-mail address. It may be reasonable, under the circumstances, for a recipient of the card to infer that Joe has agreed to communicate electronically for business purposes. However, in the absence of additional facts, it would not necessarily be reasonable to infer Joe’s agreement to communicate electronically for purposes outside the scope of the business indicated by use of the business card.
C. Sally may have several e-mail addresses - home, main office, office of a nonprofit organization on whose board Sally sits. In each case, it may be reasonable to infer that Sally is willing to communicate electronically with respect to business related to the business/purpose associated with the respective e-mail addresses. However, depending on the circumstances, it may not be reasonable to communicate with Sally for purposes other than those related to the purpose for which she maintained a particular e-mail account.
D. Among the circumstances to be considered in finding an agreement would be the time when the assent occurred relative to the timing of the use of electronic communications. If I order books from an on-line vendor, such as Bookseller.com my intention to conduct that transaction...
and to receive any correspondence related to the transaction, electronically can be inferred from my conduct. Accordingly, as to information related to that transaction it is reasonable for Bookseller to deal with me electronically. The examples noted above are intended to focus the inquiry on the party’s agreement to conduct a transaction electronically. Similarly, if two people are at a meeting and one tells the other to send an e-mail to confirm a transaction - the requisite agreement under subsection (b) would exist. In each case, the use of a business card, statement at a meeting, or other evidence of willingness to conduct a transaction electronically must be viewed in light of all the surrounding circumstances with a view toward broad validation of electronic transactions.

4. Just as circumstances may indicate the existence of agreement, express or implied from surrounding circumstances, circumstances may also demonstrate the absence of true agreement. For example:

A. If Automaker, Inc., were to issue a recall of automobiles via its Internet website, it would not be able to rely on this Act to validate that notice in the case of a person who never logged on to the website, or indeed, had no ability to do so, notwithstanding a clause in a paper purchase contract by which the buyer agreed to receive such notices in such a manner.

B. Buyer executes a standard form contract in which an agreement to receive all notices electronically is set forth on page 3 in the midst of other fine print. Buyer has never communicated with Seller electronically, and has not provided any other information in the contract to suggest a willingness to deal electronically. Not only is it unlikely that any but the most formalistic of agreements may be found, but nothing in this Act prevents courts from policing such form contracts under common law doctrines relating to contract formation, unconscionability and the like.

5. Subsection (c) has been added to make clear the ability of a party to refuse to conduct a transaction electronically, even if the person has conducted transactions electronically in the past. The effectiveness of a party’s refusal to conduct a transaction electronically will be determined under other applicable law in light of all surrounding circumstances.

6. Subsection (e) is an essential provision in the overall scheme of this Act. While this Act validates and effectuates electronic records and electronic signatures, the legal effect of such records and signatures is left to existing substantive law outside this Act except in very narrow circumstances. See, e.g., Section 16. Even when this Act operates to validate records and signatures in an electronic medium, it expressly preserves the substantive rules of other law applicable to such records. See, e.g., Section 11.

For example, beyond validation of records, signatures and contracts based on the medium used, Sections 7 (a) and (b) should not be interpreted as establishing the legal effectiveness of any given record, signature or contract. Where a rule of law requires that the record contain minimum substantive content, the legal effect of such a record will depend on whether the record meets the substantive requirements of other applicable law.

Section 8 expressly preserves a number of legal requirements in currently existing law relating to the presentation of information in writing. Although this Act now would allow such information to be presented in an electronic record, Section 8 provides that the other substantive requirements of law must be satisfied in the electronic medium as well.

SECTION 6. CONSTRUCTION AND APPLICATION.
This [Act] must be construed and applied:

(1) to facilitate electronic transactions consistent with other applicable law;

(2) to be consistent with reasonable practices concerning electronic transactions and with the continued expansion of those practices; and

(3) to effectuate its general purpose to make uniform the law with respect to the subject of this [Act] among States enacting it.

DRAFT COMMENTS
1. The purposes and policies of this Act are
a) to facilitate and promote commerce and governmental transactions by validating and authorizing the use of electronic records and electronic signatures;
b) to eliminate barriers to electronic commerce and governmental transactions resulting from uncertainties relating to writing and signature requirements;
c) to simplify, clarify and modernize the law governing commerce and governmental transactions through the use of electronic means;
d) to permit the continued expansion of commercial and governmental electronic practices through custom, usage and agreement of the parties;
e) to promote uniformity of the law among the states (and worldwide) relating to the use of electronic and similar technological means of effecting and performing commercial and governmental transactions;
f) to promote public confidence in the validity, integrity and reliability of electronic commerce and governmental transactions; and

g) to promote the development of the legal and business infrastructure necessary to implement electronic commerce and governmental transactions.

2. This Act has been drafted to permit flexible application consistent with its purpose to validate electronic transactions. The provisions of this Act validating and effectuating the employ of electronic media allow the courts to apply them to new and unforeseen technologies and practices. As time progresses, it is anticipated that what is new and unforeseen today will be commonplace tomorrow. Accordingly, this legislation is intended to set a framework for the validation of media which may be developed in the future and which demonstrate the same qualities as the electronic media contemplated and validated under this Act.
SECTION 7. LEGAL RECOGNITION OF ELECTRONIC RECORDS, ELECTRONIC SIGNATURES, AND ELECTRONIC CONTRACTS.

(a) A record or signature may not be denied legal effect or enforceability solely because it is in electronic form.
(b) A contract may not be denied legal effect or enforceability solely because an electronic record was used in its formation.
(c) If a law requires a record to be in writing, an electronic record satisfies the law.
(d) If a law requires a signature, an electronic signature satisfies the law.

Source: UNCITRAL Model Law on Electronic Commerce, Articles 5, 6, and 7.

DRAFT COMMENTS

1. This section sets forth the fundamental premise of this Act: namely, that the medium in which a record, signature, or contract is created, presented or retained does not affect it’s legal significance. Subsections (a) and (b) are designed to eliminate the single element of medium as a reason to deny effect or enforceability to a record, signature, or contract. The fact that the information is set forth in an electronic, as opposed to paper, record is irrelevant.

2. Under Restatement 2d Contracts Section 8, a contract may have legal effect and yet be unenforceable. Indeed, one circumstance where a record or contract may have effect but be unenforceable is in the context of the Statute of Frauds. Though a contract may be unenforceable, the records may have collateral effects, as in the case of a buyer that insures goods purchased under a contract unenforceable under the Statute of Frauds. The insurance company may not deny a claim on the ground that the buyer is not the owner, though the buyer may have no direct remedy against seller for failure to deliver. See Restatement 2d Contracts, Section 8, Illustration 4.

While this section would validate an electronic record for purposes of a statute of frauds, if an agreement to conduct the transaction electronically cannot reasonably be found (See Section 5(b)), then a necessary predicate to the applicability of this Act would be absent and this Act would not validate the electronic record. Whether the electronic record might be valid under other law is not addressed by this Act.

3. Subsections (c) and (d) provide the positive assertion that electronic records and signatures satisfy legal requirements for writings and signatures. The provisions are limited to requirements in laws that a record be in writing or be signed. This section does not address requirements imposed by other law in addition to requirements for writings and signatures. See, e.g., Section 8.

Subsections (c and d) are particularized applications of subsection (a). The purpose is to validate and effectuate electronic records and signatures as the equivalent of writings, subject to all of the rules applicable to the efficacy of a writing, except as such other rules are modified by the more specific provisions of this Act.

Illustration 1: A sends the following e-mail to B: “I hereby offer to buy widgets from you, delivery next Tuesday. /s/ A” B responds with the following e-mail: “I accept your offer to buy widgets for delivery next Tuesday, /s/ B” The e-mails may not be denied effect solely because they are electronic. In addition, the e-mails do qualify as records under the Statute of Frauds. However, because there is no quantity stated in either record, the parties’ agreement would be unenforceable under existing UCC Section 2-201(1).

Illustration 2: A sends the following e-mail to B: “I hereby offer to buy 100 widgets for $1000, delivery next Tuesday. /s/ A” B responds with the following e-mail: “I accept your offer to purchase 100 widgets for $1000, delivery next Tuesday. /s/ B” In this case the analysis is the same as in Illustration 1 except that here the records otherwise satisfy the requirements of UCC Section 2-201(1). The transaction may not be denied legal effect solely because there is not a pen and ink “writing” or “signature”.

4. Section 8 addresses additional requirements imposed by other law which may affect the legal effect or enforceability of an electronic record in a particular case. For example, in section 8(a) the legal requirement addressed is the provision of information in writing. The section then sets forth the standards to be applied in determining whether the provision of information by an electronic record is the equivalent of the provision of information in writing. The requirements in section 8 are in addition to the bare validation that occurs under this section.

5. Under the substantive law applicable to a particular transaction within this Act, the legal effect of an electronic record may be separate from the issue of whether the record contains a signature. For example, where notice must be given as part of a contractual obligation, the effectiveness of the notice will turn on whether the party provided the notice regardless of whether the notice was signed (See Section 15). An electronic record attributed to a party under Section 9 and complying with the requirements of Section 15, would suffice in that case, notwithstanding that it may not contain an electronic signature.

SECTION 8. PROVISION OF INFORMATION IN WRITING; PRESENTATION OF RECORDS.

(a) If parties have agreed to conduct a transaction by electronic means and a law requires a person to provide, send, or deliver information in writing to another person, the requirement is satisfied if the information is provided, sent, or delivered, as the case may be, in an electronic record capable of retention by the recipient at the time of receipt. An electronic record is not capable of retention by the recipient if the sender or its information processing system inhibits the ability of the recipient to print or store the electronic record.

(b) If a law other than this [Act] requires a record (i) to be posted or displayed in a certain manner, (ii) to be sent, communicated, or transmitted by a specified method, or (iii) to contain information that is formatted in a certain manner, the following rules apply:

(1) The record must be posted or displayed in the manner specified in the other law.
(2) Except as otherwise provided in subsection (d)(2), the record must be sent, communicated, or transmitted by the method specified in the other law.

(3) The record must contain the information formatted in the manner specified in the other law.

(c) If a sender inhibits the ability of a recipient to store or print an electronic record, the electronic record is not enforceable against the recipient.

(d) The requirements of this section may not be varied by agreement, but:

(1) to the extent a law other than this [Act] requires information to be provided, sent, or delivered in writing but permits that requirement to be varied by agreement, the requirement under subsection (a) that the information be in the form of an electronic record capable of retention may also be varied by agreement; and

(2) a requirement under a law other than this [Act] to send, communicate, or transmit a record by [first-class mail, postage prepaid] [regular United States mail], may be varied by agreement to the extent permitted by the other law.

Source: Canadian - Uniform Electronic Commerce Act

DRAFT COMMENTS

1. This section is a savings provision, designed to assure, consistent with the fundamental purpose of this act, that otherwise applicable substantive law will not be overridden by this Act. The section makes clear that while the pen and ink provisions of such other law may be satisfied electronically, nothing in this Act vitiates the other requirements of such laws. The section addresses a number of issues related to disclosures and notice provisions in other laws.

2. This section is independent of the prior section. Section 7 refers to legal requirements for a writing. This section refers to legal requirements for the provision of information in writing or relating to the method or manner of presentation or delivery of information. The section addresses more specific legal requirements of other laws, provides standards for satisfying the more particular legal requirements, and defers to other law for satisfaction of requirements under those laws.

3. Under subsection (a), to meet a requirement of other law that information be provided in writing, the recipient of an electronic record of the information must be able to get to the electronic record and read it, and must have the ability to get back to the information in some way at a later date. Accordingly, the section requires that the electronic record be capable of retention for later review.

The section specifically provides that any inhibition on retention imposed by the sender or the sender’s system will preclude satisfaction of this section because electronic information may be given to a person in a manner which prevents the person from retaining a copy of the information. The policies underlying laws requiring the provision of information in writing warrant the imposition of an additional burden on the sender to make the information available in a manner which will permit subsequent reference. A difficulty does exist for senders of information because of the disparate systems of their recipients and the capabilities of those systems. Certainly where the sender or sender’s system imposes an inhibition on retention by the recipient, this section has not been satisfied. It is left for the courts to determine whether the sender has complied with this section if evidence demonstrates that it is the recipient’s system which precludes subsequent reference to the information.

4. Subsection (b) is a savings provision for laws which provide for the means of delivering or displaying information and which are not affected by the Act. For example, if a law requires delivery of notice by first class U.S. mail, that means of delivery would not be affected by this Act. The information to be delivered may be provided on a disc, i.e., in electronic form, but the particular means of delivery must still be via the U.S. postal service. Display, delivery and formatting requirements will continue to be applicable to electronic records and signatures. If those legal requirements can be satisfied in an electronic medium, e.g., the information can be presented in 20 point bold type as required by other law, this Act will validate the use of the medium, leaving to the other applicable law the question of whether the particular electronic record meets the other legal requirements. If a law requires that particular records be delivered together, or attached to other records, this Act does not preclude the delivery of the records together in an electronic communication, so long as the records are connected or associated with each other in a way determined to satisfy the other law.

5. Subsection (c) provides incentives for senders of information to use systems which will not inhibit the other party from retaining the information. However, there are circumstances where a party providing certain information may wish to inhibit retention in order to protect intellectual property rights or prevent the other party from retaining confidential information about the sender. In such cases inhibition is understandable, but if the sender wishes to enforce the record in which the information is contained, the sender may not inhibit its retention by the recipient. Unlike subsection (a), subsection (c) applies in all transactions and simply provides for unenforceability against the recipient. Subsection (a) applies only where another law imposes the writing requirement, and subsection (a) imposes a broader responsibility on the sender to assure retention capability by the recipient.

6. The protective purposes of this section justify the non-waivability provided by Subsection (d). However, since the requirements for sending and formatting and the like are imposed by other law, to the extent other law permits waiver of such protections, there is no justification for imposing a more severe burden in an electronic environment.

SECTION 9. ATTRIBUTION AND EFFECT OF ELECTRONIC RECORD AND ELECTRONIC SIGNATURE.

(a) An electronic record or electronic signature is attributable to a person if it was the act of the person. The act of the person may be shown in any manner, including a showing of the efficacy of any security procedure applied
to determine the person to which the electronic record or electronic signature was attributable.

(b) The effect of an electronic record or electronic signature attributed to a person under subsection (a) is determined from the context and surrounding circumstances at the time of its creation, execution, or adoption, including the parties’ agreement, if any, and otherwise as provided by law.

DRAFT COMMENTS

1. Under subsection (a), so long as the electronic record or electronic signature resulted from a person’s action it will be attributed to that person - the legal effect of that attribution is addressed in subsection (b). This section does not alter existing rules of law regarding attribution. The section assures that such rules will be applied in the electronic environment. A person’s actions include actions taken by human agents of the person, as well as actions taken by an electronic agent, i.e., the tool, of the person. Although the rule may appear to state the obvious, it assures that the record or signature is not ascribed to a machine, as opposed to the person operating or programming the machine.

In each of the following cases, both the electronic record and electronic signature would be attributable to a person under subsection (a):

A. The person types his/her name as part of an e-mail purchase order;
B. The person’s employee, pursuant to authority, types the person’s name as part of an e-mail purchase order;
C. The person’s computer, programmed to order goods upon receipt of inventory information within particular parameters, issues a purchase order which includes the person’s name, or other identifying information, as part of the order.

In each of the above cases, law other than this Act would ascribe both the signature and the action to the person if done in a paper medium. Subsection (a) expressly provides that the same result will occur when an electronic medium is used.

2. Nothing in this section affects the use of a signature as a device for attributing a record to a person. Indeed, a signature is often the primary method for attributing a record to a person. In the foregoing examples, once the electronic signature is attributed to the person, the electronic record would also be attributed to the person, unless the person established fraud, forgery, or other invalidating cause. However, a signature is not the only method for attribution.

3. In the context of attribution of records, normally the content of the record will provide the necessary information for a finding of attribution. It is also possible that an established course of dealing between parties may result in a finding of attribution. Just as with a paper record, evidence of forgery or counterfeiting may be introduced to rebut the evidence of attribution.

The use of facsimile transmissions provides a number of examples of attribution using information other than a signature. A facsimile may be attributed to a person because of the information printed across the top of the page that indicates the machine from which it was sent. Similarly, the transmission may contain a letterhead which identifies the sender. Some cases have held that the letterhead actually constituted a signature because it was a symbol adopted by the sender with intent to authenticate the facsimile. However, the signature determination resulted from the necessary finding of intention in that case. Other cases have found facsimile letterheads NOT to be signatures because the requisite intention was not present. The critical point is that with or without a signature, information within the electronic record may well suffice to provide the facts resulting in attribution of an electronic record to a particular party.

4. Certain information may be present in an electronic environment that does not appear to attribute but which clearly links a person to a particular record. Numerical codes, personal identification numbers, public and private key combinations, all serve to establish the party to whom an electronic record should be attributed. Of course security procedures will be another piece of evidence available to establish attribution.

The inclusion of a specific reference to security procedures as a means of proving attribution is salutary because of the unique importance of security procedures in the electronic environment. In certain processes, a technical and technological security procedure may be the best way to convince a trier of fact that a particular electronic record or signature was that of a particular person. In certain circumstances, the use of a security procedure to establish that the record and related signature came from the person’s business might be necessary to overcome a claim that a hacker intervened. The reference to security procedures is not intended to suggest that other forms of proof of attribution should be accorded less persuasive effect. It is also important to recall that the particular strength of a given procedure does not affect the procedure’s status as a security procedure, but only affects the weight to be accorded the evidence of the security procedure as tending to establish attribution.

5. This section does apply in determining the effect of a “click-through” transaction. A “click-through” transaction involves a process which, if executed with an intent to “sign,” will be an electronic signature directly covered. See definition of Electronic Signature. In the context of an anonymous “click-through”, issues of proof will be paramount. This section will be relevant to establish that the resulting electronic record is attributable to a particular person upon the requisite proof, including security procedures which may track the source of the click-through.

6. Once it is established that a record or signature is attributable to a particular party, the effect of a record or signature must be determined in light of the context and surrounding circumstances, including the parties’ agreement, if any. Also informing the effect of any attribution will be other legal requirements considered in light of the context. Subsection (b) addresses the effect of the record or signature once attributed to a person.
SECTION 10. EFFECT OF CHANGE OR ERROR. If a change or error in an electronic record occurs in a transmission between parties to a transaction, the following rules apply:

1. If the parties have agreed to use a security procedure to detect changes or errors and one party has conformed to the procedure, but the other party has not, and the nonconforming party would have detected the change or error had that party also conformed, the conforming party may avoid the effect of the changed or erroneous electronic record.

2. In an automated transaction involving an individual, the individual may avoid the effect of an electronic record that resulted from an error made by the individual in dealing with the electronic agent of another person if the electronic agent did not provide an opportunity for the prevention or correction of the error and, at the time the individual learns of the error, the individual:
   (A) promptly notifies the other person of the error and that the individual did not intend to be bound by the electronic record received by the other person;
   (B) takes reasonable steps, including steps that conform to the other person's reasonable instructions, to return to the other person or, if instructed by the other person, to destroy the consideration received, if any, as a result of the erroneous electronic record; and (C) has not used or received any benefit or value from the consideration, if any, received from the other person.

3. If neither paragraph (1) nor paragraph (2) applies, the change or error has the effect provided by other law, including the law of mistake, and the parties' contract, if any.

4. Paragraphs (2) and (3) may not be varied by agreement.

Source: Restatement 2d Contracts, Sections 152-155.

DRAFT COMMENTS

1. This section is limited to changes and errors occurring in transmissions between parties - whether person-person (paragraph 1) or in an automated transaction involving an individual and a machine (paragraphs 1 and 2). The section focuses on the effect of changes and errors occurring when records are exchanged between parties. In cases where changes and errors occur in contexts other than transmission, the law of mistake is expressly made applicable to resolve the conflict.

The section covers both changes and errors. For example, if Buyer sends a message to Seller ordering 100 widgets, but Buyer's information processing system changes the order to 1000 widgets, a “change” has occurred between what Buyer transmitted and what Seller received. If on the other hand, Buyer typed in 1000 intending to order only 100, but sent the message before noting the mistake, an error would have occurred which would also be covered by this section.

2. Paragraph (1) deals with any transmission where the parties have agreed to use a security procedure to detect changes and errors. It operates against the nonconforming party, i.e., the party in the best position to have avoided the change or error, regardless of whether that person is the sender or recipient. The source of the error/change is not indicated, and so both human and machine errors/changes would be covered. With respect to errors or changes that would not be detected by the security procedure even if applied, the parties are left to the general law of mistake to resolve the dispute.

3. Paragraph (1) applies only in the situation where a security procedure would detect the error/change but one party fails to use the procedure and does not detect the error/change. In such a case, consistent with the law of mistake generally, the record is made avoidable at the instance of the party who took all available steps to avoid the mistake. See Restatement 2d Contracts Section 152-154.

Making the erroneous record avoidable by the conforming party is consistent with Sections 153 and 154 of the Restatement 2d Contracts because the nonconforming party was in the best position to avoid the problem, and would bear the risk of mistake. Such a case would constitute mistake by one party. The mistaken party (the conforming party) would be entitled to avoid any resulting contract under Section 153 because s/he does not have the risk of mistake and the nonconforming party had reason to know of the mistake.

4. As with paragraph (1), paragraph (2), when applicable, allows the mistaken party to avoid the effect of the erroneous electronic record. However, the subsection is limited to human error on the part of an individual when dealing with the electronic agent of the other party. In a transaction between individuals there is a greater ability to correct the error before parties have acted on it. However, when an individual makes an error while dealing with the electronic agent of the other party, it may not be possible to correct the error before the other party has shipped or taken other action in reliance on the erroneous record.

Paragraph (2) applies only to errors made by individuals. If the error results from the electronic agent it would constitute a system error. In such a case the effect of that error would be resolved under paragraph (1) if applicable, otherwise under paragraph (3) and the general law of mistake.

5. The party acting through the electronic agent/machine is given incentives by this section to build in safeguards which enable the individual to prevent the sending of an erroneous record, or correct the error once sent. For example, the electronic agent may be programmed to provide a “confirmation screen” to the individual setting forth all the information the individual initially approved. This would provide the individual with the ability to prevent the erroneous record from ever being sent. Similarly, the electronic agent might receive the record sent by the individual and then send back a confirmation which the individual must again accept before the transaction is completed. This would allow for correction of an erroneous record. In either case, the electronic agent would “provide an opportunity for prevention or correction of the error; and the subsection would not apply.

6. Paragraph (2) also places additional requirements on the mistaken individual before the paragraph may be
invoked to avoid an erroneous electronic record. The individual must take prompt action to advise the other party of the error and the fact that the individual did not intend the electronic record. Whether the action is prompt must be determined from all the circumstances including the individual’s ability to contact the other party. The individual should advise the other party both of the error and of the lack of intention to be bound (i.e., avoidance) by the electronic record received. Since this provision allows avoidance by the mistaken party, that party should also be required to expressly note that it is seeking to avoid the electronic record, i.e., lacked the intention to be bound.

Second, restitution is normally required in order to undo a mistaken transaction. Accordingly, the individual must also return or destroy any consideration received, adhering to instructions from the other party in any case. This is to assure that the other party retains control over the consideration sent in error.

Finally, and most importantly in regard to transactions involving intermediaries which may be harmed because transactions cannot be unwound, the individual cannot have received any benefit from the transaction. This section prevents a party from unwinding a transaction after the delivery of value and consideration which cannot be returned or destroyed. For example, if the consideration received is information, it may not be possible to avoid the benefit conferred. While the information itself could be returned, mere access to the information, or the ability to redistribute the information would constitute a benefit precluding the mistaken party from unwinding the transaction. It may also occur that the mistaken party receives consideration which changes in value between the time of receipt and the first opportunity to return. In such a case restitution cannot be made adequately, and the transaction would not be avoidable. In each of the foregoing cases, under subparagraph (2)(c), the individual would have received the benefit of the consideration and would NOT be able to avoid the erroneous electronic record.

7. In all cases not covered by paragraphs (1) or (2), where error or change to a record occur, the parties contract, or other law, specifically including the law of mistake, applies to resolve any dispute. If the error occurs in the context of record retention, Section12 will apply. In that case the standard is one of accuracy and retrievability of the information.

8. Paragraph (4) makes the error correction provision in paragraph (2) and the application of the law of mistake in paragraph (3) nonvariable. Paragraph (2) provides incentives for parties using electronic agents to establish safeguards for individuals dealing with them. It also avoids unjustified windfalls to the individual by erecting stringent requirements before the individual may exercise the right of avoidance under the paragraph. Therefore, there is no reason to permit parties to avoid the paragraph by agreement. Rather, parties should satisfy the paragraph’s requirements.

SECTION 11. NOTARIZATION AND ACKNOWLEDGMENT. If a law requires a signature or record to be notarized, acknowledged, verified, or made under oath, the requirement is satisfied if the electronic signature of the person authorized to perform those acts, together with all other information required to be included by other applicable law, is attached to or logically associated with the signature or record.

DRAFT COMMENTS

This Section permits a notary public and other authorized officers to act electronically, effectively removing the stamp/seal requirements. However, the section does not eliminate any of the other requirements of notarial laws, and consistent with the entire thrust of this Act, simply allows the signing and information to be accomplished in an electronic medium.

For example, Buyer wishes to send a notarized Real Estate Purchase Agreement to Seller via e-mail. The notary must appear in the room with the Buyer, satisfy him/herself as to the identity of the Buyer, and swear to that identification. All that activity must be reflected as part of the electronic Purchase Agreement and the notary’s electronic signature must appear as a part of the electronic real estate purchase contract.

As another example, Buyer seeks to send Seller an affidavit averring defects in the products received. A court clerk, authorized under state law to administer oaths, is present with Buyer in a room. The Clerk administers the oath and includes the statement of the oath, together with any other requisite information, in the electronic record to be sent to the Seller. Upon administering the oath and witnessing the application of Buyer’s electronic signature to the electronic record, the Clerk also applies his electronic signature to the electronic record. So long as all substantive requirements of other applicable law have been fulfilled and are reflected in the electronic record, the sworn electronic record of Buyer is as effective as if it had been transcribed on paper.

SECTION 12. RETENTION OF ELECTRONIC RECORDS; ORIGINALS.

(a) If a law requires that a record be retained, the requirement is satisfied by retaining an electronic record of the information in the record which:

(1) accurately reflects the information set forth in the record after it was first generated in its final form as an electronic record or otherwise; and

(2) remains accessible for later reference.

(b) A requirement to retain a record in accordance with subsection (a) does not apply to any information the sole purpose of which is to enable the record to be sent, communicated, or received.

(c) A person may satisfy subsection (a) by using the services of another person if the requirements of that subsection are satisfied.

(d) If a law requires a record to be presented or retained in its original form, or provides consequences if the
record is not presented or retained in its original form, that law is satisfied by an electronic record retained in accordance with subsection (a).

(e) If a law requires retention of a check, that requirement is satisfied by retention of an electronic record of the information on the front and back of the check in accordance with subsection (a).

(f) A record retained as an electronic record in accordance with subsection (a) satisfies a law requiring a person to retain a record for evidentiary, audit, or like purposes, unless a law enacted after the effective date of this [Act] specifically prohibits the use of an electronic record for the specified purpose.

(g) This section does not preclude a governmental agency of this State from specifying additional requirements for the retention of a record subject to the agency’s jurisdiction.

Source: UNICITRAL Model Law on Electronic Commerce Articles 8 and 10.

DRAFT COMMENTS

1. This section deals with the serviceability of electronic records as retained records and originals. So long as there exists reliable assurance that the electronic record accurately reproduces the information, this section continues the theme of establishing the functional equivalence of electronic and paper-based records. This is consistent with Fed.R.Evid. 1001(3) and Unif.R.Evid. 1001(3) (1974). This section assures that information stored electronically will remain effective for all audit, evidentiary, archival and similar purposes.

2. In an electronic medium, the concept of an original document is problematic. For example, as one drafts a document on a computer the “original” is either on a disc or the hard drive to which the document has been initially saved. If one periodically saves the draft, the fact is that at times a document may be first saved to disc then to hard drive, and at others vice versa. In such a case the “original” may change from the information on the disc to the information on the hard drive. Indeed, it may be argued that the “original” exists solely in RAM and, in a sense, the original is destroyed when a “copy” is saved to a disc or to the hard drive. In any event, in the context of record retention, the concern focuses on the integrity of the information, and not with its “originality.”

3. Subsection (a) requires accuracy and the ability to access at a later time. The requirement of accuracy is derived from the Uniform and Federal Rules of Evidence. The requirement of continuing accessibility addresses the issue of technology obsolescence and the need to update and migrate information to developing systems. It is not unlikely that within the span of 5-10 years (a period during which retention of much information is required) a corporation may evolve through one or more generations of technology. More to the point, this technology may be incompatible with each other necessitating the reversion of information from one system to the other.

For example, certain operating systems from the early 1980’s, e.g., memory typewriters, became obsolete with the development of personal computers. The information originally stored on the memory typewriter would need to be converted to the personal computer system in a way meeting the standards for accuracy contemplated by this section. It is also possible that the medium on which the information is stored is less stable. For example, information stored on floppy discs is generally less stable, and subject to a greater threat of disintegration, that information stored on a computer hard drive. In either case, the continuing accessibility issue must be satisfied to validate information stored by electronic means under this section.

This section permits parties to convert original written records to electronic records for retention so long as the requirements of subsection (a) are satisfied. Accordingly, in the absence of specific requirements to retain written records, written records may be destroyed once saved as electronic records satisfying the requirements of this section.

The subsection refers to the information contained in an electronic record, rather than relying on the term electronic record, as a matter of clarity that the critical aspect in retention is the information itself. What information must be retained is determined by the purpose for which the information is needed. If the addressing and pathway information regarding an e-mail is relevant, then that information should also be retained. However, if it is the substance of the e-mail that is relevant, only that information need be retained. Of course, wise record retention would include all such information since what information will be relevant at a later time will not be known.

4. Subsections (b) and (c) simply make clear that certain ancillary information or the use of third parties, does not affect the serviceability of records and information retained electronically. Again, the relevance of particular information will not be known until that information is required at a subsequent time.

5. Subsection (d) continues the theme of the Act as validating electronic records as originals where the law requires retention of an original. The validation of electronic records and electronic information as originals is consistent with the Uniform Rules of Evidence. See Uniform Rules of Evidence 1001(3), 1002, 1003 and 1004.

6. Subsection (e) specifically addresses particular concerns regarding check retention statutes in many jurisdictions. A Report compiled by the Federal Reserve Bank of Boston identifies hundreds of state laws which require the retention or production of original canceled checks. Such requirements preclude banks and their customers from realizing the benefits and efficiencies related to truncation processes otherwise validated under current law. The benefits to banks and their customers from electronic check retention are effectuated by this provision.

7. Subsections (f) and (g) generally address other record retention statutes. As with check retention, all businesses and individuals may realize significant savings from electronic record retention. So long as the standards in Section 12 are satisfied, this section permits all parties to obtain those benefits. As always the government may require
records in any medium, however, these subsections require a governmental agency to specifically identify the types of records and requirements that will be imposed.

SECTION 13. ADMISSIBILITY IN EVIDENCE. In a proceeding, evidence of a record or signature may not be excluded solely because it is in electronic form.

Source: UNICITRAL Model Law on Electronic Commerce Article 9.

DRAFT COMMENT
Like section 7, this Section prevents the nonrecognition of electronic records and signatures solely on the ground of the media in which information is presented.

Nothing in this section relieves a party from establishing the necessary foundation for the admission of an electronic record. See Uniform Rules of Evidence 1001(3), 1002,1003 and 1004.

SECTION 14. AUTOMATED TRANSACTION. In an automated transaction, the following rules apply:

1. A contract may be formed by the interaction of electronic agents of the parties, even if no individual was aware of or reviewed the electronic agents' actions or the resulting terms and agreements.

2. A contract may be formed by the interaction of an electronic agent and an individual, acting on the individual’s own behalf or for another person, including by an interaction in which the individual performs actions that the individual is free to refuse to perform and which the individual knows or has reason to know will cause the electronic agent to complete the transaction or performance.

3. The terms of the contract are determined by the substantive law applicable to it.

Source: UNICITRAL Model Law on Electronic Commerce Article 11.

DRAFT COMMENTS
1. This section confirms that contracts can be formed by machines functioning as electronic agents for parties to a transaction. It negates any claim that lack of human intent, at the time of contract formation, prevents contract formation. When machines are involved, the requisite intention flows from the programming and use of the machine. As in other cases, these are salutary provisions consistent with the fundamental purpose of the Act to remove barriers to electronic transactions while leaving the substantive law, e.g., law of mistake, law of contract formation, unaffected to the greatest extent possible.

2. The process in paragraph (2) validates an anonymous click-through transaction. It is possible that an anonymous click-through process may simply result in no recognizable legal relationship, e.g., A goes to a person’s website and acquires access without in any way identifying herself, or otherwise indicating agreement or assent to any limitation or obligation, and the owner's site grants A access. In such a case no legal relationship has been created.

On the other hand it may be possible that A’s actions indicate agreement to a particular term. For example, A goes to a website and is confronted by an initial screen which advises her that the information at this site is proprietary, that A may use the information for her own personal purposes, but that, by clicking below, A agrees that any other use without the site owner’s permission is prohibited. If A clicks “agree” and downloads the information and then uses the information for other, prohibited purposes, should not A be bound by the click? It seems the answer properly should be, and would be, yes.

If the owner can show that the only way A could have obtained the information was from his website, and that the process to access the subject information required that A must have clicked the “I agree” button after having the ability to see the conditions on use, A has performed actions which A was free to refuse, which A knew would cause the site to grant her access, i.e., “complete the transaction.” The terms of the resulting contract will be determined under general contract principles, but will include the limitation on A’s use of the information, as a condition precedent to granting her access to the information.

3. In the transaction set forth in Comment 2, the record of the transaction also will include an electronic signature. By clicking “I agree” A adopted a process with the intent to “sign,” i.e., bind herself to a legal obligation, the resulting record of the transaction. If a “signed writing” were required under otherwise applicable law, this transaction would be enforceable. If a “signed writing” were not required, it may be sufficient to establish that the electronic record is attributable to A under section 9. Attribution may be shown in any manner reasonable including showing that, of necessity, A could only have gotten the information through the process at the website.

SECTION 15. TIME AND PLACE OF SENDING AND RECEIPT.

(a) Unless otherwise agreed between the sender and the recipient, an electronic record is sent when it:

1. is addressed properly or otherwise directed properly to an information processing system that the recipient has designated or uses for the purpose of receiving electronic records or information of the type sent and from which the recipient is able to retrieve the electronic record;

2. is in a form capable of being processed by that system; and

3. enters an information processing system outside the control of the sender or of a person that sent the electronic record on behalf of the sender or enters a region of the information processing system designated or used by the recipient which is under the control of the recipient.

(b) Unless otherwise agreed between a sender and the recipient, an electronic record is received when:

1. it enters an information processing system that the recipient has designated or uses for the purpose of receiving electronic records or information of the type sent and
from which the recipient is able to retrieve the electronic record; and
(2) it is in a form capable of being processed by that system.

(c) Subsection (b) applies even if the place the information processing system is located is different from the place the electronic record is deemed to be received under subsection (d).

(d) Unless otherwise expressly provided in the electronic record or agreed between the sender and the recipient, an electronic record is deemed to be sent from the sender’s place of business and to be received at the recipient’s place of business. For purposes of this subsection, the following rules apply:

(1) If the sender or recipient has more than one place of business, the place of business of that person is the place having the closest relationship to the underlying transaction.

(2) If the sender or the recipient does not have a place of business, the place of business is the sender’s or recipient’s residence, as the case may be.

(e) An electronic record is received under subsection (b) even if no individual is aware of its receipt.

(f) Receipt of an electronic acknowledgment from an information processing system described in subsection (b) establishes that a record was received but, by itself, does not establish that the content sent corresponds to the content received.

(g) If a person is aware that an electronic record purportedly sent under subsection (a), or purportedly received under subsection (b), was not actually sent or received, the legal effect of the sending or receipt is determined by other applicable law. Except to the extent permitted by the other law, the requirements of this subsection may not be varied by agreement.

Source: UNCITRAL Model Law on Electronic Commerce Article 15.

DRAFT COMMENTS

1. This section provides default rules regarding when and from where an electronic record is sent and when and where an electronic record is received. This section does not address the efficacy of the record that is sent or received. That is, whether a record is unintelligible or unusable by a recipient is a separate issue from whether that record was sent or received. The effectiveness of an illegible record, whether it binds any party, are questions left to other law.

2. Subsection (a) furnishes rules for determining when an electronic record is sent. The effect of the sending and its import are determined by other law once it is determined that a sending has occurred.

In order to have a proper sending, the subsection requires that information be properly addressed or otherwise directed to the recipient. In order to send within the meaning of this section, there must be specific information which will direct the record to the intended recipient. Although mass electronic sending is not precluded, a general broadcast message, sent to systems rather than individuals, would not suffice as a sending.

The record will be considered sent once it leaves the control of the sender, or comes under the control of the recipient. Records sent through e-mail or the Internet will pass through many different server systems. Accordingly, the critical element when more than one system is involved is the loss of control by the sender.

However, the structure of many message delivery systems is such that electronic records may actually never leave the control of the sender. For example, within a university or corporate setting, e-mail sent within the system to another faculty member is technically not out of the sender’s control since it never leaves the organization’s server. Accordingly, to qualify as a sending, the e-mail must arrive at a point where the recipient has control. The effect of an electronic record that is thereafter “pulled back,” e.g., removed from a mailbox, is not addressed by this section. The analog in the paper world would be removing a letter from a person’s mailbox. As in the case of providing information electronically under Section 8, the recipient’s ability to receive a message should be judged from the perspective of whether the sender has done any action which would preclude retrieval. This is especially the case in regard to sending, since the sender must direct the record to a system designated or used by the recipient.

3. Subsection (b) provides simply that when a record enters the system which the recipient has designated or uses and to which it has access, in a form capable of being processed by that system, it is received. By keying receipt to a system which is accessible by the recipient, the issue of a recipient leaving messages with a server or other service to avoid receipt, is removed. However, the issue of how the sender proves the time of receipt is not resolved by this section.

To assure that the recipient retains control of the place of receipt, subsection (b) requires that the system be specified or used by the recipient, and that the system be used or designated for the type of record being sent. Many people have multiple e-mails for different purposes, and the purpose is to assure that recipients can designate the e-mail address or system to be used in a particular transaction. For example, the recipient retains the ability to designate a home e-mail for personal matters, work e-mail for official business, or a separate organizational e-mail solely for the business purposes of that organization. If A sends B a notice at his home which relates to business, it may not be deemed received if B designated his business address as the sole address for business purposes. Actual knowledge upon seeing it at home would qualify as receipt under the otherwise applicable substantive law.

4. Subsections (c) and (d) provide default rules for determining where a record will be considered to have been sent or received. The focus is on the place of business of the recipient and not the physical location of the information processing system, which may bear absolutely no relation to the transaction between the parties. It is not uncommon for users of electronic commerce to communicate from one State to another without knowing the location of information systems through which communication is
operated. In addition, the location of certain communication systems may change without either of the parties being aware of the change. Accordingly, where the place of sending or receipt is an issue under other applicable law, e.g., conflict of laws issues, tax issues, the relevant location should be the location of the sender or recipient and not the location of the information processing system.

Subsection (d) assures individual flexibility in designating the place from which a record will be considered sent or at which a record will be considered received. Under subsection (d) a person may designate the place of sending or receipt unilaterally in an electronic record. This ability, as with the ability to designate by agreement, may be limited by otherwise applicable law to places having a reasonable relationship to the transaction.

5. Subsection (e) makes clear that receipt is not dependent on a person having notice that the record is in the person’s system. Receipt occurs when the record reaches the designated system whether or not the recipient ever retrieves the record. The paper analog is the recipient who never reads a mail notice.

6. Subsection (f) provides legal certainty regarding the effect of an electronic acknowledgment. It only addresses the fact of receipt, not the quality of the content, nor whether the electronic record was read or “opened.”

7. Subsection (g) limits the parties’ ability to vary the method for sending and receipt provided in subsections (a) and (b), when there is a legal requirement for the sending or receipt. As in other circumstances where legal requirements derive from other substantive law, to the extent that the other law permits variation by agreement, this Act does not impose any additional requirements, and provisions of this Act may be varied to the extent provided in the other law.

SECTION 16. TRANSFERABLE RECORDS.

(a) In this section, “transferable record” means an electronic record that:

(1) would be a note under [Article 3 of the Uniform Commercial Code] or a document under [Article 7 of the Uniform Commercial Code] if the electronic record were in writing; and

(2) the issuer of the electronic record expressly has agreed is a transferable record.

(b) A person has control of a transferable record if a system employed for evidencing the transfer of interests in the transferable record reliably establishes that person as the person to which the transferable record was issued or transferred.

(c) A system satisfies subsection (b), and a person is deemed to have control of a transferable record, if the transferable record is created, stored, and assigned in such a manner that:

(1) a single authoritative copy of the transferable record exists which is unique, identifiable, and, except as otherwise provided in paragraphs (4), (5), and (6), unalterable;

(2) the authoritative copy identifies the person asserting control as:

(A) the person to which the transferable record was issued; or

(B) if the authoritative copy indicates that the transferable record has been transferred, the person to which the transferable record was most recently transferred;

(3) the authoritative copy is communicated to and maintained by the person asserting control or its designated custodian;

(4) copies or revisions that add or change an identified assignee of the authoritative copy can be made only with the consent of the person asserting control;

(5) each copy of the authoritative copy and any copy of a copy is readily identifiable as a copy that is not the authoritative copy; and

(6) any revision of the authoritative copy is readily identifiable as authorized or unauthorized.

(d) Except as otherwise agreed, a person having control of a transferable record is the holder, as defined in [Section 1-201(20) of the Uniform Commercial Code], of the transferable record and has the same rights and defenses as a holder of an equivalent record or writing under [the Uniform Commercial Code], including, if the applicable statutory requirements under [Section 3-302(a), 7-501, or 9-308 of the Uniform Commercial Code] are satisfied, the rights and defenses of a holder in due course, a holder to which a negotiable document of title has been duly negotiated, or a purchaser, respectively. Delivery, possession, and endorsement are not required to obtain or exercise any of the rights under this subsection.

(e) Except as otherwise agreed, an obligor under a transferable record has the same rights and defenses as an equivalent obligor under equivalent records or writings under [the Uniform Commercial Code].

(f) If requested by a person against which enforcement is sought, the person seeking to enforce the transferable record shall provide reasonable proof that the person is in control of the transferable record. Proof may include access to the authoritative copy of the transferable record and related business records sufficient to review the terms of the transferable record and to establish the identity of the person having control of the transferable record.

Source: Revised Article 9, Section 9-105.

DRAFT COMMENTS

1. Paper negotiable instruments and documents are unique in the fact that a tangible token - a piece of paper - actually embodies intangible rights and obligations. The extreme difficulty of creating a unique electronic token which embodies the singular attributes of a paper negotiable document or instrument, dictates that the rules relating to negotiable documents and instruments not be simply amended to allow the use of an electronic record for the requisite paper writing. However, the desirability of establishing rules by which business parties might be able to acquire some of the benefits of negotiability in an electronic environment is recognized by the inclusion of this Section on Transferable Records.
This section provides legal support for the creation, transferability and enforceability of electronic note and document equivalents, as against the issuer/obligor. The certainty created by the section provides the requisite incentive for industry to develop the systems and processes, which involve significant expenditures of time and resources, to enable the use of such electronic documents.

The importance of facilitating the development of systems which will permit electronic equivalents is a function of cost, efficiency and safety for the records. The storage cost and space needed for the billions of paper notes and documents is phenomenal. Further, natural disasters can wreak havoc on the ability to meet legal requirements for retaining, retrieving and delivering paper instruments. The development of electronic systems meeting the rigorous standards of this Section will permit retention of copies which reflect the same integrity as the original. As a result, storage and transmission costs will be reduced, while security and the ability to satisfy legal requirements governing such paper records will be enhanced.

Section 16 provides for the creation of an electronic record which may be controlled by the holder who in turn may obtain the benefits of holder in due course and good faith purchaser status. If the benefits and efficiencies of electronic media are to be realized in this industry it is essential to establish a mean by which transactions involving paper promissory notes may be accomplished completely electronically. Particularly as other aspects of such transactions are accomplished electronically, the drag on the transaction of requiring a paper note becomes evident. In addition to alleviating the logistical problems of generating and storing and retrieving such paper notes, the mailing and transmission costs associated with such transactions will also be reduced.

2. The definition of transferable record is limited in two significant ways. First, only the equivalent of paper promissory notes and paper documents of title can be created as transferable records. Notes and Documents of Title do not impact the broad systems that relate to the broader payments mechanisms related, for example, to checks. Impacting the check collection system by allowing for “electronic checks” has ramifications well beyond the ability of this Act. Accordingly, this Act excludes from its scope, transactions governed by UCC Articles 3 and 4.

The limitation to promissory note equivalents in Section 16 is quite important in that regard because of the ability to deal with many enforcement issues by contract without affecting such systemic concerns.

Second, not only is Section 16 limited to electronic records which would qualify as negotiable promissory notes or documents if they were in writing, but the issuer of the electronic record must expressly agree that the electronic record is to be considered a transferable record.

The definition of transferable record as “an electronic record that...the issuer of the electronic record expressly has agreed is a transferable record” indicates that the electronic record itself will likely set forth the issuer’s agreement, though it may be argued that a contemporaneous electronic or written record might set forth the issuer’s agreement. However, conversion of a paper note issued as such would not be possible because the issuer would not be the issuer, in such a case, of an electronic record. The purpose of such a restriction is to assure that transferable records can only be created at the time of issuance by the obligor. The possibility that a paper note might be electrofied and then intentionally destroyed was not intended to be covered by Section 16.

The requirement that the obligor expressly agree in the electronic record to its treatment as a transferable record does not otherwise affect the characterization of a transferable record (i.e., does not affect what would be a paper note) because it is a statutory condition. Further, it does not obligate the issuer to undertake to do any other act than the payment of the obligation evidenced by the transferable record. Therefore, it does not make the transferable record “conditional” within the meaning of Section 104(a)(3).

3. Under Section 16, acquisition of “control” over an electronic record serves as a substitute for “possession” in the paper analog. More precisely, “control” under Section 16 serves as the substitute for delivery, endorsement and possession of a negotiable promissory note or negotiable document of title. Section 16(b) allows control to be found so long as “a system employed for evidencing the transfer of interests in the transferable record reliably establishes [the person claiming control] as the person to which the transferable record was issued or transferred.”

The key point is that a system, whether involving third party registry or technological safeguards, must be shown to reliably establish the identity of the person entitled to payment. Section 16(c) then sets forth a safe harbor list of very strict requirements for such a system. The specific provisions listed in Section 16(c) are derived from Section 105 of Revised Article 9. Generally, the transferable record must be unique, identifiable, and except as specifically permitted, unalterable. That “authoritative copy” must (i) identify the person claiming control as the person to whom the record was issued or most recently transferred, (ii) be maintained by the person claiming control or its designee, and (iii) be unalterable except with the permission of the person claiming control. In addition any copy of the authoritative copy must be readily identifiable as a copy and all revisions must be readily identifiable as authorized or unauthorized.

The control requirements may be satisfied through the use of a trusted third party registry system. Such systems are currently in place with regard to the transfer of securities entitlements under Article 8 of the UCC, and in the transfer of cotton warehouse receipts under the program sponsored by the United States Department of Agriculture. This Act would recognize the use of such a system so long as the standards of subsection (c) were satisfied. In addition, a technological system which met such exacting standards would also be permitted under Section 16.
For example, a borrower signs an electronic record which would be a promissory note or document if it were paper. The borrower specifically agrees in the electronic record that it will qualify as a transferable record under this section. The lender implements a newly developed technological system which dates, encrypts, and stores all the electronic information in the transferable record in a manner which lender can demonstrate reliably establishes lender as the person to which the transferable record was issued. In the alternative, the lender may contract with a third party to act as a registry for all such transferable records, retaining records establishing the party to whom the record was issued and all subsequent transfers of the record. An example of this latter method for assuring control is the system established for the issuance and transfer of electronic cotton warehouse receipts under 7 C.F.R. section 735 et seq.

Of greatest importance in the system used is the ability to securely and demonstrably be able to transfer the record to others in a manner which assures that only one “holder” exists. The need for such certainty and security resulted in the very stringent standards for a system outlined in subsection (c). A system relying on a third party registry is likely the most effective way to satisfy the requirements of subsection (c) that the transferable record remain unique, identifiable and unalterable, while also providing the means to assure that the transferee is clearly noted and identified. It must be remembered that Section 16 was drafted in order to provide sufficient legal certainty regarding the rights of those in control of such electronic records, that legal incentives would exist to warrant the development of systems which would establish the requisite control. During the drafting of Section 16, representatives from the Federal Reserve carefully scrutinized the impact of any electronicization of any aspect of the national payment system. Section 16 represents a compromise position which, as noted, serves as a bridge pending more detailed study and consideration of what legal changes, if any, are necessary or appropriate in the context of the payment systems impacted. Accordingly, Section 16 provides limited scope for the attainment of important rights derived from the concept of negotiability, in order to permit the development of systems which will satisfy its strict requirements for control.

4. It is important to note what the Section does not provide. Issues related to enforceability against intermediate transferees and transferors (i.e., endorser liability under a paper note), warranty liability that would attach in a paper note, and issues of the effect of taking a transferable record on the underlying obligation, are NOT addressed by this section. Such matters must be addressed, if at all, by contract between and among the parties in the chain of transmission and transfer of the transferable record. In the event that such matters are not addressed by the contract, the issues would need to be resolved under otherwise applicable law. Other law may include general contract principles of assignment and assumption, or may include rules from Article 3 applied by analogy.

For example, Issuer agrees to pay a debt by means of a transferable record issued to A. Unless there is agreement between Issuer and A that the transferable record “suspends” the underlying obligation (see UCC Section 3-310), A would not be prevented from enforcing the underlying obligation without the transferable record. Similarly, if A transfers the transferable record to B by means granting B control, B may obtain holder in due course rights against the Obligor/Issuer, but B’s recourse against A would not be clear unless A specifically agreed to remain liable under the transferable record. Although the rules of Article 3 may be applied by analogy in an appropriate context, in the absence of agreement in the transferable record, the liability of the transferor would not be clear.

5. Current business models exist which rely for their efficacy on the benefits of negotiability. A principal example, and one which informed much of the development of Section 16, involves the mortgage backed securities industry. Aggregators of commercial paper acquire mortgage secured promissory notes following a chain of transfers beginning with the origination of the mortgage loan by a mortgage broker. In the course of the transfers of this paper, buyers of the notes and lenders/secured parties for these buyers will intervene. For the ultimate purchaser, the ability to rely on holder in due course and a good faith purchaser status creates the legal security necessary to issue its own investment securities which are backed by the obligations evidenced by the notes purchased. Only through their HIDC status can these purchasers be assured that third party claims will be barred. Only through their HIDC status can the end purchaser avoid the incredible burden of requiring and assuring that each person in the chain of transfer has waived any and all defenses to performance which may be created during the chain of transfer.

6. This Section is a stand-alone provision. Although references are made to specific provisions in Article 3, Article 7, and Article 9 of the Uniform Commercial Code, these provisions are incorporated into this Act and made the applicable rules for purposes of this Act. The rights of parties to transferable records are established under subsections (d) and (e). Subsection (d) provides rules for determining the rights of a party in control of a transferable record. The subsection makes clear that the rights are determined under this section, and not under other law, by incorporating the rules on the manner of acquisition into this statute. The last sentence of subsection (d) is intended to assure that requirements related to notions of possession, which are inherently inconsistent with the idea of an electronic record, are not incorporated into this statute. If a person establishes control, Section 16(d) provides that that person is the “holder” of the transferable record which is equivalent to a holder of an analogous paper negotiable instrument. More importantly, if the person acquired control in a manner which would make it a holder in due course of an equivalent paper record, the person acquires the rights of a HIDC. The person in control would therefore be able to enforce the transferable record against the obligor regardless of intervening claims and
defenses. However, by pulling these rights into Section 16, this Act does NOT validate the wholesale electrification of promissory notes under Article 3.

Further, it is important to understand that a transferable record under Section 16, while having no counterpart under Article 3, would likely be an “account” under Article 9. Accordingly, two separate bodies of law would apply to that asset of the obligee. A taker of the transferable record under Section 16 may acquire purchaser rights under Article 9, however, those rights may be defeated by a trustee in bankruptcy of a prior person in control unless perfection under Article 9 by filing is achieved. If the person in control also takes control in a manner granting it holder in due course status, of course that person would take free of any claim by a bankruptcy trustee or lien creditor.

7. Subsection (e) accords to the obligor of the transferable record rights equal to those of an obligor under an equivalent paper record. Accordingly, unless a waiver of defense clause is obtained in the electronic record, or the transferee obtains HDC rights under subsection (d), the obligor has all the rights and defenses available to it under a contract assignment. Additionally, the obligor has the right to have the electronic record altered or “noted” to indicate payment.

8. Subsection (f) grants the obligor the right to have the transferable record and other information made available for purposes of assuring the correct person to pay. This will allow the obligor to protect its interest and obtain the defense of discharge by payment or performance. This is particularly important because a person receiving subsequent control under the appropriate circumstances may well qualify as a holder in due course who can again enforce payment of the transferable record.

9. Section 16 is a singular exception to the thrust of this Act to simply validate electronic media used in commercial transactions. Section 16 actually provides a means for expanding electronic commerce. It provides certainty to lenders and investors regarding the enforceability of a new electronic commerce. It provides certainty to transactions. Section 16 actually provides a means for simply validating electronic media used in commercial transactions.

8. Subsection (f) grants the obligor the right to have the transferable record and other information made available for purposes of assuring the correct person to pay. This will allow the obligor to protect its interest and obtain the defense of discharge by payment or performance. This is particularly important because a person receiving subsequent control under the appropriate circumstances may well qualify as a holder in due course who can again enforce payment of the transferable record.

9. Section 16 is a singular exception to the thrust of this Act to simply validate electronic media used in commercial transactions. Section 16 actually provides a means for expanding electronic commerce. It provides certainty to lenders and investors regarding the enforceability of a new class of financial services. It is hoped that the legal protections afforded by Section 16 will engender the development of technological and business models which will permit realization of the significant cost savings and efficiencies available through electronic transacting in the financial services industry. Although only a bridge to more detailed consideration of the broad issues related to negotiability in an electronic context, Section 16 provides the impetus for that broader consideration while allowing continuation of developing technological and business models.

[SECTION 17. CREATION AND RETENTION OF ELECTRONIC RECORDS AND CONVERSION OF WRITTEN RECORDS BY GOVERNMENTAL AGENCIES. [Each governmental agency] [The [designated state officer]] of this State shall determine whether, and the extent to which, [it] [a governmental agency] will create and retain electronic records and convert written records to electronic records.]

DRAFT COMMENT: See Draft Comments following Section 19.

[SECTION 18. ACCEPTANCE AND DISTRIBUTION OF ELECTRONIC RECORDS BY GOVERNMENTAL AGENCIES.

(a) Except as otherwise provided in Section 12(f), [each governmental agency] [the [designated state officer]] of this State shall determine whether, and the extent to which, [it] [a governmental agency] will send and accept electronic records and electronic signatures to and from other persons and otherwise create, generate, communicate, store, process, use, and rely upon electronic records and electronic signatures.

(b) To the extent that a governmental agency uses electronic records and electronic signatures under subsection (a), the [governmental agency] [designated state officer], giving due consideration to security, may specify:

1. the manner and format in which the electronic records must be created, generated, sent, communicated, received, and stored and the systems established for those purposes;

2. if electronic records must be signed by electronic means, the type of electronic signature required, the manner and format in which the electronic signature must be affixed to the electronic record, and the identity of, or criteria that must be met by, any third party used by a person filing a document to facilitate the process;

3. control processes and procedures as appropriate to ensure adequate preservation, disposition, integrity, security, confidentiality, and auditability of electronic records; and

4. any other required attributes for electronic records which are specified for corresponding nonelectronic records or reasonably necessary under the circumstances.

(c) Except as otherwise provided in Section 12(f), this [Act] does not require a governmental agency of this State to use or permit the use of electronic records or electronic signatures.]

Source: Illinois Act Section 25-101; Florida Electronic Signature Act, Chapter 96-324, Section 7 (1996).

DRAFT COMMENT: See Draft Comments following Section 19.

[SECTION 19. INTEROPERABILITY. The [governmental agency] [designated officer] of this State which adopts standards pursuant to Section 18 may encourage and promote consistency and interoperability with similar requirements adopted by other governmental agencies of this and other States and the federal government and nongovernmental persons interacting with governmental agencies of this State. If appropriate, those standards may specify differing levels of standards from which governmental agencies of this State may choose in implementing the most appropriate standard for a particular application.]

DRAFT COMMENTS
1. Section 17-19 have been bracketed as optional provisions to be considered for adoption by each State. Among the barriers to electronic commerce are barriers which exist in the use of electronic media by State governmental agencies - whether among themselves or in external dealing with the private sector. In those circumstances where the government acts as a commercial party, e.g., in areas of procurement, the general validation provisions of the Act will apply. That is to say, the government must agree to conduct transactions electronically with vendors and customers of government services.

However, there are other circumstances when government ought to establish the ability to proceed in transactions electronically. Whether in regard to records and communications within and between governmental agencies, or with respect to information and filings which must be made with governmental agencies, these sections allow a state to establish the groundwork for such electronicization.

2. The provisions in Sections 17-19 are broad and very general. In many states they will be unnecessary because those states have already enacted legislation designed to facilitate governmental use of electronic records and communications. However, in many states broad validating rules are needed and desired. Accordingly, this Act provides these Sections as a baseline.

Of paramount importance in all states however, is the need for states to assure that whatever systems and rules are adopted, the systems established are compatible with the systems of other governmental agencies and with common systems in the private sector. A very real risk exists that implementation of systems by myriad governmental agencies and offices may create barriers because of a failure to consider compatibility, than would be the case otherwise.

3. The provisions in Section 17-19 are broad and general to provide the greatest flexibility and adaptation to the specific needs of the individual states. The differences and variations in the organization and structure of governmental agencies mandates this approach. However, it is imperative that each State always keep in mind the need to prevent the erection of barriers through appropriate coordination of systems and rules within the parameters set by the State.

4. Section 17 authorizes state agencies to use electronic records and electronic signatures generally for intra-governmental purposes, and to convert written records and manual signatures to electronic records and electronic signatures. By its terms the section gives enacting legislatures the option to leave the decision to use electronic records or convert written records and signatures to the governmental agency or assign that duty to a designated state officer. It also authorizes the destruction of written records after conversion to electronic form.

5. Section 18 broadly authorizes state agencies to send and receive electronic records and signatures in dealing with nongovernmental persons. Again, the provision is permissive and not obligatory (see subsection (c)). However, it does provide specifically that with respect to electronic records used for evidentiary purposes, Section 12 will apply unless a particular agency expressly opts out.

6. Section 19 is the most important section of the three. It requires governmental agencies or state officers to take account of consistency in applications and interoperability to the extent practicable when promulgating standards. This section is critical in addressing the concern that inconsistent applications may promote barriers greater than currently exist. Without such direction the myriad systems that could develop independently would be new barriers to electronic commerce, not a removal of barriers. The key to interoperability is flexibility and adaptability. The requirement of a single system may be as big a barrier as the proliferation of many disparate systems.

SECTION 20. SEVERABILITY CLAUSE. If any provision of this [Act] or its application to any person or circumstance is held invalid, the invalidity does not affect other provisions or applications of this [Act] which can be given effect without the invalid provision or application, and to this end the provisions of this [Act] are severable.

SECTION 21. EFFECTIVE DATE. This [Act] takes effect
United States Code – Government Paperwork Elimination Act

TITLE 44 - PUBLIC PRINTING AND DOCUMENTS

CHAPTER 35 - COORDINATION OF FEDERAL INFORMATION POLICY

Sec. 3501. - Purposes

The purposes of this chapter are to -

(1) minimize the paperwork burden for individuals, small businesses, educational and nonprofit institutions, Federal contractors, State, local and tribal governments, and other persons resulting from the collection of information by or for the Federal Government;

(2) ensure the greatest possible public benefit from and maximize the utility of information created, collected, maintained, used, shared and disseminated by or for the Federal Government;

(3) coordinate, integrate, and to the extent practicable and appropriate, make uniform Federal information resources management policies and practices as a means to improve the productivity, efficiency, and effectiveness of Government programs, including the reduction of information collection burdens on the public and the improvement of service delivery to the public;

(4) improve the quality and use of Federal information to strengthen decision making, accountability, and openness in Government and society;

(5) minimize the cost to the Federal Government of the creation, collection, maintenance, use, dissemination, and disposition of information;

(6) strengthen the partnership between the Federal Government and State, local, and tribal governments by minimizing the burden and maximizing the utility of information created, collected, maintained, used, disseminated, and retained by or for the Federal Government;

(7) provide for the dissemination of public information on a timely basis, on equitable terms, and in a manner that promotes the utility of the information to the public and makes effective use of information technology;

(8) ensure that the creation, collection, maintenance, use, dissemination, and disposition of information by or for the Federal Government is consistent with applicable laws, including laws relating to -

(A) privacy and confidentiality, including section 552a of title 5;

(B) security of information, including the Computer Security Act of 1987 (Public Law 100-235); and

(C) access to information, including section 552 of title 5;

(9) ensure the integrity, quality, and utility of the Federal statistical system;

(10) ensure that information technology is acquired, used, and managed to improve performance of agency missions, including the reduction of information collection burdens on the public; and

(11) improve the responsibility and accountability of the Office of Management and Budget and all other Federal agencies to Congress and to the public for implementing the information collection review process, information resources management, and related policies and guidelines established under this chapter.

Sec. 3502. - Definitions

As used in this chapter -

(1) the term “agency” means any executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the Government (including the Executive Office of the President), or any independent regulatory agency, but does not include -

(A) the General Accounting Office;

(B) Federal Election Commission;

(C) the governments of the District of Columbia and of the territories and possessions of the United States, and their various subdivisions; or

(D) Government-owned contractor-operated facilities, including laboratories engaged in national defense research and production activities;

(2) the term “burden” means time, effort, or financial resources expended by persons to generate, maintain, or provide information to or for a Federal agency, including the resources expended for -

(A) reviewing instructions;

(B) acquiring, installing, and utilizing technology and systems;

(C) adjusting the existing ways to comply with any previously applicable instructions and requirements;

(D) searching data sources;

(E) completing and reviewing the collection of information; and

(F) transmitting, or otherwise disclosing the information;

(3) the term “collection of information” -

(A) means the obtaining, causing to be obtained, soliciting, or requiring the disclosure to third parties or the public, of facts or opinions by or for an agency, regardless of form or format, calling for either -

(i) answers to identical questions posed to, or identical reporting or recordkeeping requirements imposed on, ten or more persons, other than agencies, instrumentalities, or employees of the United States; or
the term "person'' means an individual, partnership, or organization, including any association, corporation, business trust, or legal representative, an organized group of individuals, a State, territorial, tribal, or local government or branch thereof, or a political subdivision of a State, territory, tribal, or local government or a branch of a political subdivision;

(10) the term "person'' means an individual, partnership, association, corporation, business trust, or legal representative, an organized group of individuals, a State, territorial, tribal, or local government or branch thereof, or a political subdivision of a State, territory, tribal, or local government or a branch of a political subdivision;

(11) the term "practical utility'' means the ability of an agency to use information, particularly the capability to process such information in a timely and useful fashion;

(12) the term "public information'' means any information, regardless of form or format, that an agency discloses, disseminates, or makes available to the public;

(ii) answers to questions posed to agencies, instrumentalities, or employees of the United States which are to be used for general statistical purposes; and

(4) the term “Director” means the Director of the Office of Management and Budget;

(5) the term “independent regulatory agency” means the Board of Governors of the Federal Reserve System, the Commodity Futures Trading Commission, the Consumer Product Safety Commission, the Federal Communications Commission, the Federal Deposit Insurance Corporation, the Federal Energy Regulatory Commission, the Federal Housing Finance Board, the Federal Maritime Commission, the Federal Trade Commission, the Interstate Commerce Commission, the Mine Enforcement Safety and Health Review Commission, the Nuclear Regulatory Commission, the Occupational Safety and Health Review Commission, the Postal Rate Commission, the Securities and Exchange Commission, and any other similar agency designated by statute as a Federal independent regulatory agency or commission;

(6) the term “information resources” means information and related resources, such as personnel, equipment, funds, and information technology;

(7) the term “information resources management” means the process of managing information resources to accomplish agency missions and to improve agency performance, including through the reduction of information collection burdens on the public;

(8) the term “information system” means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information;

(9) the term “information technology” has the meaning given that term in section 5002 of the Clinger-Cohen Act of 1996 (40 U.S.C. 1401) but does not include national security systems as defined in section 5142 of that Act (40 U.S.C. 1452);

(10) the term “person” means an individual, partnership, association, corporation, business trust, or legal representative, an organized group of individuals, a State, territorial, tribal, or local government or branch thereof, or a political subdivision of a State, territory, tribal, or local government or a branch of a political subdivision;

(11) the term “practical utility” means the ability of an agency to use information, particularly the capability to process such information in a timely and useful fashion;

(12) the term “public information” means any information, regardless of form or format, that an agency discloses, disseminates, or makes available to the public;

(13) the term “recordkeeping requirement” means a requirement imposed by or for an agency on persons to maintain specified records, including a requirement to -

(A) retain such records;

(B) notify third parties, the Federal Government, or the public of the existence of such records;

(C) disclose such records to third parties, the Federal Government, or the public or

(D) report to third parties, the Federal Government, or the public regarding such records; and

(14) the term “penalty” includes the imposition by an agency or court of a fine or other punishment; a judgment for monetary damages or equitable relief; or the revocation, suspension, reduction, or denial of a license, privilege, right, grant, or benefit.
The authority of the Director under this chapter shall be exercised consistent with applicable law.

(b) With respect to general information resources management policy, the Director shall -

1. develop and oversee the implementation of uniform information resources management policies, principles, standards, and guidelines;

2. foster greater sharing, dissemination, and access to public information, including through -
   (A) the use of the Government Information Locator Service; and
   (B) the development and utilization of common standards for information collection, storage, processing and communication, including standards for security, interconnectivity and interoperability;

3. initiate and review proposals for changes in legislation, regulations, and agency procedures to improve information resources management practices;

4. oversee the development and implementation of best practices in information resources management, including training; and

5. oversee agency integration of program and management functions with information resources management functions.

(c) With respect to the collection of information and the control of paperwork, the Director shall -

1. review and approve proposed agency collections of information;

2. coordinate the review of the collection of information associated with Federal procurement and acquisition by the Office of Information and Regulatory Affairs with the Office of Federal Procurement Policy, with particular emphasis on applying information technology to improve the efficiency and effectiveness of Federal procurement, acquisition and payment, and to reduce information collection burdens on the public;

3. minimize the Federal information collection burden, with particular emphasis on those individuals and entities most adversely affected;

4. maximize the practical utility of and public benefit from information collected by or for the Federal Government; and

5. establish and oversee standards and guidelines by which agencies are to estimate the burden to comply with a proposed collection of information.

(d) With respect to information dissemination, the Director shall develop and oversee the implementation of policies, principles, standards, and guidelines to -

1. apply to Federal agency dissemination of public information, regardless of the form or format in which such information is disseminated; and

2. promote public access to public information and fulfill the purposes of this chapter, including through the effective use of information technology.

(e) With respect to statistical policy and coordination, the Director shall -

1. coordinate the activities of the Federal statistical system to ensure -
   (A) the efficiency and effectiveness of the system; and
   (B) the integrity, objectivity, impartiality, utility, and confidentiality of information collected for statistical purposes;

2. ensure that budget proposals of agencies are consistent with system-wide priorities for maintaining and improving the quality of Federal statistics and prepare an annual report on statistical program funding;

3. develop and oversee the implementation of Government-wide policies, principles, standards, and guidelines concerning -
   (A) statistical collection procedures and methods;
   (B) statistical data classification;
   (C) statistical information presentation and dissemination;
   (D) timely release of statistical data; and
   (E) such statistical data sources as may be required for the administration of Federal programs;

4. evaluate statistical program performance and agency compliance with Government-wide policies, principles, standards and guidelines;

5. promote the sharing of information collected for statistical purposes consistent with privacy rights and confidentiality pledges;

6. coordinate the participation of the United States in international statistical activities, including the development of comparable statistics;

7. appoint a chief statistician who is a trained and experienced professional statistician to carry out the functions described under this subsection;

8. establish an Interagency Council on Statistical Policy to advise and assist the Director in carrying out the functions under this subsection that shall -
   (A) be headed by the chief statistician; and
   (B) consist of -
   (i) the heads of the major statistical programs; and
   (ii) representatives of other statistical agencies under rotating membership; and
provide opportunities for training in statistical policy functions to employees of the Federal Government under which -

(A) each trainee shall be selected at the discretion of the Director based on agency requests and shall serve under the chief statistician for at least 6 months and not more than 1 year; and

(B) all costs of the training shall be paid by the agency requesting training.

(f) With respect to records management, the Director shall -

(1) provide advice and assistance to the Archivist of the United States and the Administrator of General Services to promote coordination in the administration of chapters 29, 31, and 33 of this title with the information resources management policies, principles, standards, and guidelines established under this chapter;

(2) review compliance by agencies with -

(A) the requirements of chapters 29, 31, and 33 of this title; and

(B) regulations promulgated by the Archivist of the United States and the Administrator of General Services;

(3) oversee the application of records management policies, principles, standards, and guidelines, including requirements for archiving information maintained in electronic format, in the planning and design of information systems.

(g) With respect to privacy and security, the Director shall -

(1) develop and oversee the implementation of policies, principles, standards, and guidelines on privacy, confidentiality, security, disclosure and sharing of information collected or maintained by or for agencies;

(2) oversee and coordinate compliance with sections 5 and 6 of the Computer Security Act of 1987 (40 U.S.C. 759 note), [1] to identify and afford security protections commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information collected or maintained by or on behalf of an agency.

(h) With respect to Federal information technology, the Director shall -

(1) in consultation with the Director of the National Institute of Standards and Technology and the Administrator of General Services -

(A) develop and oversee the implementation of policies, principles, standards, and guidelines for information technology functions and activities of the Federal Government, including periodic evaluations of major information systems; and

(B) oversee the development and implementation of standards under section 5131 of the Clinger-Cohen Act of 1996 (40 U.S.C. 1441);

(2) monitor the effectiveness of, and compliance with, directives issued under division E of the Clinger-Cohen Act of 1996 (40 U.S.C. 1401 et seq.) and directives issued under section 110 of the Federal Property and Administrative Services Act of 1949 (40 U.S.C. 757);

(3) coordinate the development and review by the Office of Information and Regulatory Affairs of policy associated with Federal procurement and acquisition of information technology with the Office of Federal Procurement Policy;

(4) ensure, through the review of agency budget proposals, information resources management plans and other means -

(A) agency integration of information resources management plans, program plans and budgets for acquisition and use of information technology; and

(B) the efficiency and effectiveness of inter-agency information technology initiatives to improve agency performance and the accomplishment of agency missions; and

(5) promote the use of information technology by the Federal Government to improve the productivity, efficiency, and effectiveness of Federal programs, including through dissemination of public information and the reduction of information collection burdens on the public.
subject: BOOKS AND RECORDS RETENTION / DESTRUCTION

NO.: IC78-10R3

DATE: October 5, 1998

This circular cancels and replaces Information Circular 78-10R2 dated July 14, 1989, and Information Circular 78-10R2(SR) dated February 10, 1995. This update adds information about new legislation that requires computer records to be kept in an electronically readable format even when a paper copy of the record(s) has been kept.

1. The circular gives information and guidance to persons who are required by law to keep records and books of account according to sections 230 and 230.1 of the Income Tax Act, section 87 of the Employment Insurance Act, and section 24 of the Canada Pension Plan. It does not reflect the requirements imposed by other statutes, whether federal, provincial, or municipal, to maintain adequate records and books of account.

2. The sections and subsections referred to in this circular are from the Income Tax Act. Parallel provisions for most of these matters exist in the Employment Insurance Act and Canada Pension Plan. Where significant differences do exist, they are indicated.

WHO HAS TO KEEP BOOKS AND RECORDS?

3. For the purpose of this circular, person has the meaning assigned by subsection 248(1) of the Income Tax Act (the Act). Therefore, a person in this context includes a corporation, a trust, and any exempt entity listed in subsection 149(1) of the Act such as a registered charity, a registered Canadian amateur athletic association, and a nonprofit organization.

4. Books and records must be kept by every:
   - person carrying on a business;
   - person who is required to pay or collect taxes or other amounts according to the Acts mentioned in 1 above;
   - registered charity or registered Canadian amateur athletic association; and
   - registered agent of a registered political party or an official agent for a candidate in a federal election.

RECORDS TO BE KEPT

5. For the purpose of this circular, a RECORD has the meaning assigned by subsection 248(1) of the Act. A “record” includes an account, an agreement, a book, a chart or table, a diagram, a form, an image, an invoice, a letter, a map, a memorandum, a plan, a return, a statement, a telegram, a voucher, and any other thing containing information, whether in writing or in any other form."

6. As a general rule, the Department does not specify the records and books to be kept. However, records and books of account have to:
   - permit the taxes payable or the taxes or other amounts to be collected, withheld, or deducted by a person to be determined;
   - substantiate the qualification of registered charities or registered Canadian amateur athletic association for registration under the Act;
   - permit the verification of all charitable, athletic, and political donations received for which a deduction or tax credit is available; and
   - be supported by source documents that verify the information in the records and books of account.

7. A SOURCE DOCUMENT includes items such as sales invoices, purchase invoices, cash register receipts, formal written contracts, credit card receipts, delivery slips, deposit slips, work orders, dockets, cheques, bank statements, tax returns, and general correspondence.

LOCATION OF RECORDS

8. The records and books of account have to be kept at the person’s place of business or residence in Canada or another place designated by the Minister and have to, upon request, be made available to officers of Revenue Canada for audit purposes at all reasonable times. Records and books of account kept outside Canada and accessed electronically from Canada are not records and books of account in Canada. Access to electronic records means direct, physical contact to the medium on which the record is stored (e.g., tape, disc, CD-ROM).

METHODS OF KEEPING RECORDS

9. KEEPING RECORDS AND BOOKS OF ACCOUNT pertains to a system of recording financial and other information. For example, records are considered to be kept electronically when information is directly entered into any device for electronic processing, manipulation, and/or storage on electronic or optical media and reproduction to paper.

10. Revenue Canada recognizes as records and books of account:
     - the traditional records and books of account (including supporting source documents) produced and retained in paper format; and
     - records and books produced and retained in an electronically readable format that can be related back to the supporting source documents and which are supported by a system capable of producing accessible and readable copy.

WAYS OF KEEPING RECORDS

11. A person who is required to keep records and books is responsible for keeping the records and books in a way that will ensure the trustworthiness and readability of the information recorded.
12. All records and books of account (including source documents) that originate in paper format have to be kept except where an acceptable imaging or microfilming program, as discussed in the following section, is in place. Paper format includes paper source documents from which data is entered into an electronic record-keeping system.

13. A person who is required to keep records and who records them electronically has to keep the records in an electronically readable format. This means that a person who uses computerized systems to generate records and/or books of account must keep the electronic records, even when a hard copy is kept.

14. This person should ensure that proper back-up records are maintained at all times. If any electronic records required to be maintained are lost, destroyed, or damaged, the person must report this situation to the Director of the local tax services office and recreate the files within a reasonable period of time.

IMAGING

15. Source documents and records that are in an electronically readable format must be kept in addition to the microfilm and/or electronic image.

16. ELECTRONIC IMAGE means the representation of a source record that can be used to generate an intelligible reproduction of that record, or the reproduction itself, where:
   - the reproduction is made with the intention of standing in place of the source record;
   - the interpretation of the reproduction, for the purposes for which it is being used, gives the same information as the source record; and
   - the limitations of the reproduction (e.g., resolution, tonal, or hues) are well defined and do not obscure significant details.

Paper source documents may be disposed and their images kept as permanent records.

17. Imaging and microfilm (including microfiche) reproductions of books of original entry and source documents have to be produced, controlled, and maintained according to the national standard of Canada, as outlined in the publication called Microfilm and Electronic Images as Documentary Evidence. This publication, identified as CAN/CGSB-72.11-93, is available from:

   Canadian General Standards Board
   Sales Centre
   Phase 3, 6B1
   Place du Portage
   11 Laurier St.
   Hull QC K1A 0S5
   Telephone number for calls from the Ottawa area: (819) 956-0425

   Toll-free telephone number for calls from other parts of Canada: 1-800-665-2472
   Fax number: (819) 956-5644

18. An acceptable imaging program requires that:
   (a) someone in the organization has confirmed in writing that the program will be part of the usual and ordinary activity of the organization’s business;
   (b) systems and procedures are established and documented;
   (c) a logbook is kept showing:
       - the date of imaging;
       - the signatures of the persons authorizing and performing the imaging;
       - a description of the records imaged; and
       - whether source documents are destroyed or disposed of after imaging, and the date a source document was destroyed or disposed of;
   (d) the imaging software maintains an index to permit the immediate location of any record, and the software inscribes the imaging date and the name of the person who does the imaging;
   (e) the images are of commercial quality and are legible and readable when displayed on a computer screen or reproduced on paper;
   (f) a system of inspection and quality control is established to ensure that c), d), and e) above are maintained; and
   (g) after reasonable notification, equipment in good working order is available to view, or where feasible, to reproduce a hard copy of the image.

ELECTRONIC RECORDS

19. Documentation describing physical, environmental, and system controls that exist or existed to prevent unauthorized alteration or loss of the records have to be maintained. This would also include flowcharts and policy/procedure manuals or instructions to document the flow and treatment of transactions through the accounting system from initiation to closure and storage.

20. The electronic records must show an audit trail from the source document(s), whether paper or electronic, to the financial accounts. Where no paper source document(s) exist, as in a transaction covered by a trading partner agreement of electronic data interchange (EDI), the electronic record(s) including functional acknowledgments have to be kept. It is the record keeper’s responsibility to ensure the trustworthiness and readability of EDI transaction records.

21. Retained records should be stored in a way that is appropriate to the media on which the information is recorded. Information recorded on rewritable media such as computer hard disks should be backed up on tape or other suitable medium to avoid accidental deletion or erasure of the recorded information. The media containing the recorded
information should be stored in an environment free from magnetic fields, direct light, and excessive heat.

22. A person who keeps records electronically is not relieved of any of the record keeping, readability, retention, and access responsibilities because he or she contracts out the record keeping function to a third party such as through a time share, service bureau, or other such arrangements. Therefore, the person must ensure that these requirements are met in the event of system changes by the third party, bankruptcy of the third party, or a change from one third party to another third party or from a third party to an in-house record keeping system. The record keeper is also responsible for keeping electronic records and providing access to authorized persons when a value added network (VAN) is used as an intermediary/mailbox, regardless of where the VAN is located.

23. A person who uses turnkey or packaged software to keep books and records electronically is not relieved of the responsibility to keep adequate electronic records because of deficiencies in the software. In cases where the software backup procedures are deficient, additional specific back-up procedures may be required to retain adequate electronic records. Documentation must be kept at a level of detail that will describe the data entry procedures, reports produced, and any features that alter standard reports or create new reports.

24. Where electronically kept records are converted from one format to another, it is the record keeper’s responsibility to ensure that the converted records are trustworthy and readable. The conversion must not result in a loss, destruction, or alteration of information and data relevant to the determination of taxes payable, collected, or withheld.

25. The Department is prepared to offer advice on keeping, maintaining, retaining, and storing electronic records. You can get this advice from your tax services office. This advice should not be considered or viewed as an audit, inspection, or a ruling issued by the Department. The record keeper is responsible for keeping, maintaining, retaining, and safeguarding records.

26. Subsection 230(4.2) of the Income Tax Act provides that the Minister may exempt a person or a class of persons from the requirement to keep electronic records under terms and conditions that are acceptable to the Minister.

27. The Department occasionally enters into agreements to keep specific files of electronic records to be used during subsequent audits. These agreements are referred to as RECORD RETENTION AGREEMENTS. The files under these agreements should be kept for the statutory period referred to in paragraph 30 below.

RETENTION PERIOD

28. Records and books of account have to be kept for the period or periods provided by subsections 230(4) to (7) and Part 5800 of the Income Tax Regulations or until the Minister gives written permission for their disposal. Failure to comply with this requirement could result in prosecution by the Department.

29. Subsection 230(4.1) requires every person who keeps records electronically to retain them in an electronically readable format for the retention period outlined in subsection 230(4).

30. Under the Act, books, records, and their related accounts and source documents, other than those referred to in paragraphs 29 above, have to be kept for a minimum of six years from the end of the last tax year to which they relate. The tax year is the fiscal period for corporations and the calendar year for all other taxpayers. Under the Employment Insurance Act and Canada Pension Plan, the retention period begins at the end of the calendar year to which the books and records relate.

31. The prescribed retention periods for certain books, records, and their related accounts and source documents are specified in Regulation 5800 (see Appendix). The required retention periods can be summarized as follows:

- for a corporation, two years from the date of the dissolution of the corporation (in the case of corporations that amalgamate or merge, books and records have to be retained on the basis that the new corporation is a continuation of each amalgamating corporation);
- for any nonincorporated business, six years from the end of the tax year in which the business ceased;
- for the duplicate donation receipts of a registered charity or registered Canadian amateur athletic association, other than receipts for donations of property to be held for a period of not less than ten years, two years from the end of the calendar year in which the donations were made;
- for other specified records of registered charities and registered Canadian amateur athletic associations, two years from the date the registration is revoked; and
- for records relating to political contributions, two years from the end of the calendar year to which they relate.

There are no similar provisions in the Employment Insurance Act or Canada Pension Plan.

32. Exceptions to the rules outlined in paragraphs 28 and 29 above are:

- The Minister may exempt a person or class of persons from the requirement to keep records electronically according to subsection 230(4.2).
- Books of account and records may be destroyed at an earlier time than outlined elsewhere in this circular if the Minister gives written permission for their disposal. To get such permission, a person can use Form T137, Request for Destruction of Books and Records, or can apply in writing to the Director of his or her tax services office. A written request, signed by the person or an authorized representative, should provide the following information:
- a clear identification of books, records, or other documents to be destroyed;
- the tax years for which the request applies;
- details of any special circumstances which would justify destroying the books and records at an earlier time than that normally permitted; and
- any other pertinent information.
- The Minister may, by registered letter or by a demand served personally by a representative of the Department, require specific records to be kept for an additional period of time stipulated in the letter or demand.
- If a return required by section 150 of the Act is filed late, the books and records referred to in paragraph 30 above must be kept for six years from the day the return is filed.
- Every book and record necessary for dealing with a notice of objection or appeal must be kept until the notice of objection or appeal is disposed of and the time for filing any further appeal has expired.
- In the case of paragraph 31 above, only the books and records of a deceased taxpayer or a trust can be destroyed upon receipt of a clearance certificate issued according to subsection 159(2) concerning the distribution of all property.

When Revenue Canada gives permission to destroy records and books, this permission applies only to information required to be kept under the legislation administered by Revenue Canada, and does not imply permission to destroy any books and records required to be kept under any other legislation, or by any other department or government agency.

33. The minimum retention period for the records referred to in paragraph 30 above is generally determined by the last tax year when a record may be required for purposes of the Act, and not the year when the transaction occurred and the record was created. For example, records supporting the acquisition and capital cost of investments and other capital property held by a person (including registered charities and registered Canadian amateur athletic associations) should be maintained until the day that is six years from the end of the last tax year in which such an acquisition could enter into any calculation for income tax purposes.

INADEQUATE RECORDS

34. If a person has failed to keep adequate records and books of account, subsection 230(3) provides that the Minister can specify what records or books of account shall be kept.

35. If Revenue Canada finds that records and books of account are inadequate, the Department will ordinarily request a written agreement that books and records be maintained as required. Within a reasonable period of time, usually not less than a month, the Department will follow up the request by letter or visit to ensure compliance.

36. If there has been no compliance within the time allowed, the Department will issue a formal requirement letter. The letter describes the information to be recorded in the books and describes the legal consequences and penalties for failing to comply. Failure to comply with the letter within a specified period of time may result in prosecution by the Department. On summary conviction, and in addition to any penalty otherwise payable, a taxpayer is liable to a fine of not less than $1,000, or both the fine and imprisonment. No such minimum is required under the Employment Insurance Act or the Canada Pension Plan.

37. A person who destroys or otherwise disposes of records or books of account to evade the payment of tax is subject to prosecution according to section 239. Information Circular 73-10, Tax evasion, discusses Department policies on tax evasion.

APPENDIX

PART LVIII - KEEPING BOOKS AND RECORDS

5800. (1) For the purposes of paragraph 230(4)(a) of the Act, the required retention periods for records and books of account of a person are prescribed as follows:

(a) in respect of

(i) any record of the minutes of meetings of the directors of a corporation,
(ii) any record of the minutes of meetings of the shareholders of a corporation,
(iii) any record of a corporation containing details with respect to the ownership of the shares of the capital stock of the corporation and any transfers thereof,
(iv) the general ledger or other book of final entry containing the summaries of the year-to-year transactions of a corporation, and
(v) any special contracts or agreements necessary to an understanding of the entries in the general ledger or other book of final entry referred to in subparagraph (iv), the period ending on the day that is two years after the day that the corporation is dissolved;

(b) in respect of all records and books of account that are not described in paragraph (a) of a corporation that is dissolved and in respect of the vouchers and accounts necessary to verify the information in such records and books of account, the period ending on the day that is two years after the day that the corporation is dissolved;

(c) in respect of

(i) the general ledger or other book of final entry containing the summaries of the year-to-year transactions of a business of a person (other than a corporation), and
(ii) any special contracts or agreements necessary to an understanding of the entries in the general ledger or other book of final entry referred to in subparagraph (i), the period ending on the day that is six years after the last day of the taxation year of the person in which the business ceased;
d) in respect of
(i) any record of the minutes of meetings of the executive of a registered charity or registered Canadian amateur athletic association,
(ii) any record of the minutes of meetings of the members of a registered charity or registered Canadian amateur athletic association,
(iii) all documents and by-laws governing a registered charity or registered Canadian amateur athletic association, and
(iv) all records of any donations received by a registered charity that were subject to a direction by the donor that the property given be held by the charity for a period of not less than 10 years, the period ending on the day that is two years after the date on which the registration of the registered charity or the registered Canadian amateur athletic association under the Act is revoked;

(e) in respect of all records and books of account that are not described in paragraph (d) and that relate to a registered charity or registered Canadian amateur athletic association whose registration under the Act is revoked, and in respect of the vouchers and accounts necessary to verify the information in such records and books of account, the period ending on the day that is two years after the date on which the registration of the registered charity or the registered Canadian amateur athletic association under the Act is revoked;

(f) in respect of duplicates of receipts for donations (other than donations referred to in subparagraph (d)(iv)) that are received by a registered charity or registered Canadian amateur athletic association and are required to be kept by that charity or association pursuant to subsection 230(2) of the Act, the period ending on the day that is two years from the end of the last calendar year to which the receipts relate; and

(g) notwithstanding paragraphs (c) to (f), in respect of all records, books of account, vouchers and accounts of a deceased taxpayer or a trust in respect of which a clearance certificate is issued pursuant to subsection 159(2) of the Act with respect to the distribution of all the property of such deceased taxpayer or trust, the period ending on the day that the clearance certificate is issued.

(2) For the purposes of subsection 230.1(3) of the Act, with respect to the application of paragraph 230(4)(a) of the Act, the required retention period for records and books of account that are required to be kept pursuant to section 230.1 of the Act is prescribed to be the period ending on the day that is two years after the end of the last calendar year to which the records or books of account relate.
Australian Tax Office

TR 97/21
FOI status: May be released
Taxation Ruling
Income tax: record keeping - electronic records

Preamble
This Ruling, to the extent that it is capable of being a ‘pub-
lic ruling’ in terms of Part IVAAA of the Taxation
Administration Act 1953, is a public ruling for the pur-
poses of that Part. Taxation Ruling TR 92/1 explains when
a Ruling is a public ruling and how it is binding on the
Commissioner.

What this Ruling is about
Class of person/arrangement

1. This Ruling explains to a person, including a company,
carrying on a business, the principles associated with the
retention of electronic records for the purposes of section
262A of the Income Tax Assessment Act 1936 (‘the Act’).
Where the person uses a computer, either partly or fully,
to run an accounting system, this Ruling sets out our
views on what are sufficient electronic records to be
retained to record and explain all transactions and other
acts engaged in by such a person for the purposes of the
Act. This Ruling also sets out our views on access to elec-
tronic records under section 263 of the Act.

2. Although section 262A applies for any purpose of the
Act, this Ruling considers the section as it relates to the
income and expenditure of a person carrying on a business.

3. This Ruling is the third in a series of Rulings released
by the Australian Taxation Office (‘the ATO’) on record
keeping. The first Ruling is Taxation Ruling TR 96/7 on
the general principles of record keeping. The second in
the series is Taxation Ruling TR 96/11 that sets out our
views on what records are sufficient for the purposes of
section 262A to record income from taxi takings. The
ATO has also issued a publication called ‘A Guide to
Keeping Your Business Records’. The Rulings and publi-
cation provide further information to a person carrying
on a business on their record keeping responsibilities and
should be read in conjunction with this Ruling.

4. This Ruling does not deal with the retention of electron-
ic records created from business transactions carried out
through the Internet or through the use of Smartcards.

Definitions

5. In this Ruling:

‘documents and records’ means all documents and records
including those documents and records kept in electronic
form in a computer or in other electronic storage media;

‘paper records’ means all written documentation,
whether in hand writing or by typewriter, computer or
other means of recording on paper;

‘imaging’ means the scanning of an image into a digitised
form to be stored electronically;

‘electronically’ means held or processed by means of a
computer;

‘electronic storage medium’ includes hard disc, remov-
able hard disc, diskette, floppy disc, CD-ROM, optical
disc or magnetic tapes; and

‘EDI’ means Electronic Data Interchange.

Ruling
Computerised record keeping systems

6. When a person carrying on a business chooses to
process and keep records in electronic form, the records
must be in a form that ATO staff can access and under-
stand in order to ascertain the person’s taxation liability.
Under section 25A of the Acts Interpretation Act 1901 the
person can choose at any time to satisfy access requests by
providing a hard or printed copy of their electronic
records and where necessary, system documentation,
notwithstanding that the person’s business records may
be kept electronically.

7. The information contained in a record kept in a com-
puterised accounting system is generally the same as
would be contained in a manual accounting system.

8. We acknowledge that there are risks associated with the
processing and retention of records on a computer sys-
tem that are not generally associated with manual record
keeping. Those risks include:

- the inadvertent destruction or corruption of electronic
  records;
- the unauthorised tampering with electronic records; and
- the possibility that electronic records and operating sys-
tems will become obsolete due to the constant upgrading
  or changing of computer systems over time.

System controls

9. We consider that a person carrying on a business with
a computerised accounting system generally has a series
of adequate controls available to safeguard the security
and integrity of the records processed and kept in that
system. These can include:

- access controls;
- input and output controls;
- processing controls; and
- back-up controls.

10. The ATO considers that the level of controls required
by a business is a matter for the particular business to
determine provided it can demonstrate that the records
kept in the computer system are secure and accurate.

11. We have included as Appendix A of this Ruling a
checklist of the electronic records that, providing ade-
quate controls are in place, a person carrying on a business could keep to explain the essential features (i.e., the date, amount and character) of every transaction and enable the person’s taxation liability to be ascertained. The checklist is provided as a guide only. Depending on the nature and size of the business, not all of the records listed may be applicable.

Storage of paper records in electronic form

12. A business using either a manual or a computerised accounting system may want to store and keep paper records in electronic form. Where paper records are produced or received in the course of carrying on business, the ATO accepts the imaging of those records onto an electronic storage medium provided that the electronic copies are a true and clear reproduction of the original paper records.

13. Where paper records are imaged and stored electronically the requirements of section 262A are satisfied if they are:

- not altered or manipulated once stored;
- retained for the statutory period of five years; and
- capable of being retrieved and read at all times by ATO staff.

The ATO considers that paper records imaged and stored electronically should be:

- read only; and
- subject to adequate back-up control, i.e., a duplicate back-up copy of the stored records must be kept at all times at a safe location.

Paper records that can be imaged and stored include:

- invoices, purchase orders, receipts, vouchers, credit notes, delivery dockets, etc.;
- bank statements and other bank records and documents; and
- any other paper source documents produced or received in the course of carrying on a business.

Original paper records that have been imaged onto an electronic storage medium need not be retained for the purposes of the Act.

System documentation

14. To ensure that the records are being maintained in accordance with subsections 262A(1), (3) and (4), a person should have an understanding of their computer system. System documents should be retained to explain the basic aspects of the system so ATO officers can ascertain that the system is doing what it is claimed to do.

15. Where systems (regardless of their level of sophistication) have changed over time, records are to be kept to allow the original data to be reconstructed to satisfy section 262A. The records to be kept include:

- a chronological record and explanation of all changes or upgrades to the software and hardware employed in the system, including explanations of how the new system can recreate an original record;
- where applicable, explanations of migrations of data that may have taken place across either software or hardware;
- a detailed, documented record of the controls which maintain the integrity of the old system and of the records processed and transmitted; and
- explanations of archival and back-up facilities under that system.

Any data held under an old system is to be capable of conversion to a form that is readily readable and retrievable by the ATO. Thus, the ATO would prefer that data be converted to a standard data format, e.g., ASCII, DBF or a spreadsheet format.

Access to computer records

16. Under section 263 of the Act, the Commissioner or any duly authorised officer has the right of full and free access to all buildings, places and documents, including electronically stored records required for the purposes of the Act. The provision enables an authorised officer to access and copy records held on an electronic storage medium.

17. In addition, subsection 263(3) requires the occupier of a building or place to provide an authorised officer with all reasonable facilities and assistance for the effective exercise of powers under the section. In the context of electronically stored records, reasonable facilities and assistance extend, where necessary, to the provision of login codes, keys, passwords, etc., and access to printed copies of the records as well as allowing the authorised officer to read computer and software manuals.

18. Where it is necessary to download electronic records onto ATO computers, it is the policy of the ATO to invite taxpayers to carry out the copying of these electronic records for and on behalf of the ATO on tapes or disks provided by the ATO. Where this is inconvenient or impractical, the ATO undertakes, with the approval of the taxpayers, to carry out that downloading process.

Electronic data interchange

19. Many businesses transfer data and information electronically to both internal and external sources. This process is commonly referred to as Electronic Data Interchange (‘EDI’). A special feature of EDI is that most of the transfers are done automatically between respective computers.

20. Where a person carrying on a business uses EDI, we consider section 262A requires the person to keep records that explain all EDI transactions that are relevant for any purpose of the Act. The record keeping requirements for EDI are the same as for other computer records as set out in the preceding paragraphs of this Ruling.
Date of effect

21. This Ruling applies to years commencing both before and after its date of issue.

Explanations

Electronic records

22. Records made by and stored in a computer are recognised as documents for the purposes of Commonwealth legislation. Section 25 of the Acts Interpretation Act 1901 extends the ordinary meaning of the word record to include information stored by means of a computer. The reference in subsection 262A(1) of the Act to the keeping of records therefore includes a reference to information stored or recorded by means of a computer. A person carrying on a business must keep documents and records made by and/or stored in a computer system. By virtue of subsection 262A(3), the person is required to keep these computer records in the English language or in a form readily convertible into English. The explanatory memorandum to the Taxation Laws Amendment Bill (No 5) 1989 that introduced subsection 262A(3) into the Act explained:

‘Subsection 262A(3) obliges a person who is required by the section to keep records, to keep those records:

• by paragraph (a) - in the English language or, if not in written form (e.g., in an electronic medium such as magnetic tape or computer disc), in a form which is readily accessible and convertible into writing in English; ...

23. In addition, the admissibility of computer produced evidence in Federal Courts is now governed by various provisions in the Commonwealth Evidence Act 1995 (‘the Evidence Act’). Broadly speaking, computer documents are admissible evidence in taxation matters subject to relevance and, where necessary, proof as to the competence of the computer device. Even prior to the introduction of the Evidence Act, documents held in electronic form had been accepted as admissible evidence: DFC of T v. Capron 93 ATC 4144; (1993) 25 ATR 142.

24. The ATO has for some time recognised that advances in technology have meant that many taxpayers now process and keep their accounting records electronically. We acknowledge that there are many advantages associated with such an approach. However, the ATO’s concern is that the records, whether kept on paper or electronically, must be kept accurately so as to enable that person’s liability to be readily ascertained.

25. Under section 25A of the Acts Interpretation Act 1901, where a person who keeps business records of information by means of a computer is required to produce those records under the access provisions contained in the Act, the person can choose to satisfy the access request by providing the ATO with a hard or printed copy of the electronic records in a form capable of being understood by the ATO. In some circumstances, a hard copy of system documentation explaining how the system works also needs to be made available so the ATO can ensure that the records kept in the system are correct and maintained in accordance with subsections 262A(1), (3) and (4). Paragraphs 14 and 15 of the Ruling part of this Ruling and paragraphs 31 and 32 of the Explanations part deal with the range of system documentation required to be retained.

Computerised record keeping systems

26. There are many similarities between a manual accounting system and one run by a computer. Essentially, both systems involve the updating of a general ledger and subsidiary ledgers. Many businesses use computerised accounting packages to process their financial transactions and to prepare their periodical accounts. Different businesses have different needs in terms of the type and level of complexity of the computerised accounting system they wish to operate. Some small businesses find it adequate to operate from a basic accounting system, e.g., from a computerised cash flow system where the computer acts merely as an accumulator and produces various reports at regular intervals. Other businesses need to operate from highly sophisticated and fully integrated real-time systems where one single transaction or entry in the system triggers the processing and recording of many other transactions, e.g., where a sale transaction will simultaneously update various ledger accounts, adjust stock levels, etc. We consider that computerised accounting systems operate essentially in the same manner as manual accounting systems and the records kept in them are, in principle, the same as those kept under manual accounting systems.

System controls

27. Significant concerns that the ATO has about the retention of electronic records are the risk of loss of integrity or corruption of those records and the inability over time of taxpayers to reconstruct records that have been inadvertently destroyed, manipulated or tampered with, or altered or lost within a computerised accounting system. It is normal practice for a person operating such a system in a business to safeguard the security and integrity of the records kept in that system through the use of system controls. Those commonly expected to be in place include:

• access controls, i.e., the controls over access to a computer system by some form of identification, such as a password, card system, personal identification number (‘PIN’) or some combination of these;
• input and output controls, i.e., the controls which ensure the accuracy and security of the information received and transmitted;
• processing controls, i.e., the controls which protect and ensure the integrity of the information processed by the system; and
• back-up controls, i.e., the controls that guarantee the retention of back-up copies of computer files, computer programs and the recovery of computer records in case of system failure.
28. The size of a business often dictates the level of sophistication of the computerised accounting system that the business adopts. This, in turn, impacts on the level of complexity of the system controls in place. The ATO takes the view that the levels of controls required by a business are a matter entirely for the business to determine after assessing its own requirements, provided that the records kept in the computer system are secure and accurate.

29. We stated in Taxation Ruling TR 96/7 that, in circumstances where records of individual transactions provide no additional information about the essential features of the transactions, a person can record and explain those transactions by recording and explaining groups of transactions, i.e., in the form of summary records. The same conclusion applies to records held electronically. For example, in TR 96/7, we advised that rolls of cash register tapes may be discarded after one month, provided there had been a reconciliation of the Z-totals with actual cash and bankings for that period. In this case, an electronic reconciliation, as described above, would be acceptable to the ATO provided that the reconciliation is kept for the statutory period of five years.

Storage of paper records in electronic form

30. The ATO considers that where it is intended to convert original paper records to microfilm or computer-output microfiche, the conversion needs to be carried out in such a manner that the film/fiche represents a true and clear reproduction of the original documentation. The ATO acknowledges that microfilm/microfiche technology, although not entirely obsolete, is not commonly utilised these days and that the conversion of paper records onto an electronic storage medium, by way of an imaging process, has effectively replaced that technology. The ATO therefore accepts the imaging of paper records provided the conversion process produces electronic copies that are a complete, true and clear reproduction of the original paper records. For instance, Optical Character Recognition conversion processes that do not produce a 100% accurate reproduction of original documents are not acceptable to the ATO.

System documentation

31. Where a person keeps records within a computerised accounting system, the ATO may require an explanation of the basic aspects of the computer system. To that end, certain system documents are to be retained to assist ATO officers to ascertain that the system is doing what it is claimed to do. In the case of a simple accounting software package, these documents may be limited to a system manual that explains:

- the operation of the various components of the system;
- the controls built in the system; and
- the flow of data from input to output.

32. With a sophisticated computerised accounting system, the documents need to include:

- details of the file organisation and controls;
- details of record contents, context and structure;
- the program logic, in the case of computer programs produced in-house; and
- audit trails or logs of records added, deleted and amended that relate to the accounting system.

Electronic data interchange

33. EDI is widely understood to mean the transfer of data, by agreed message standards, electronically from computer to computer. The exchange of information can be by way of document transfer only (i.e., where a document is merely sent electronically to a receiver, not unlike an invoice sent by mail) or by interactive mode (i.e., where the document results from an actual exchange of information, not unlike an interaction by telephone).

34. The ATO considers that there should be no difference in the general principles governing the records processed and kept in an EDI environment and in a normal computerised accounting system. Taxpayers who operate in an EDI environment ordinarily have in place, for their own purposes, adequate controls to safeguard the security and integrity of their transactions. Those controls have been discussed earlier.

35. Users of EDI should ensure that controls are in place to prevent unauthorised access to their EDI network by the use of access passwords, or some other form of authentication (e.g., electronic signatures), together with a secure user profile that would define the identities of the trading partners, the transaction types that can be exchanged, the standards and versions used and the direction of the exchange. This profile would ordinarily be encrypted and, in turn, secured against unlawful access by the use of user passwords, PIN numbers or access keys. In addition, EDI messages should be protected against unauthorised reading by the use of encryption techniques applied to all or part of the messages. Providing that these controls are in place, we consider that the retention requirements as stated previously in this Ruling apply equally in an EDI environment.

36. A copy of all original transmitted and received messages in their own interchanged image (e.g., EDIFACT or ANSI X12 image) is required, as well as audit trails, and logs of all EDI transactions are to be retained. The audit trails allow a transaction to be traced through a system forward to its ultimate destination and backward to its beginning through relevant source transactions. Where messages have been encrypted, those encryptions must be capable of being removed to allow for authorised officers to understand the contents of the message.

Examples

Example 1

The facts
37. Joe's Corner Mini Mart is a small family business with an annual turnover of about $300,000. Its sales are strictly on a cash basis and are recorded through a cash register. It purchases its supplies either by cash or on 30-day terms. The business pays its expense accounts either by cash from the till (for small expenses) or through a business cheque account for items of stock and other expenses. It employs one casual employee for after school and weekend hours. The employee has access to the cash register but not to the computer system that only Joe operates.

The system

38. Joe has adopted an electronic cashbook system because of the nature and size of his business. Although he is the only one who operates the system, he has built into it a password control to stop unauthorised access to his accounts. The system provides him with up-to-date information on what payments he has made (by cash or cheque) for stock or running expenses; daily total receipts he has banked and reconciled with his cash register tapes; a bank reconciliation showing deposits made and any withdrawals; periodical trial balances; income and expense reports; and even a balance sheet.

39. Joe can download these reports on a computer disk or print out a copy for his accountant or bank manager at any time. On advice from his software provider, at the end of every month Joe backs up all his accounts onto a floppy disk, which he keeps at home in case the computer system crashes. He has been provided with a system manual by his computer company and a short hands-on training session on the operation of the system. He keeps invoices sent to him by suppliers and bank statements of his business account in paper form in a filing cabinet. He also keeps a purchase order book to order stock.

Our view

40. We consider that Joe has appropriate system controls, including file back-up facilities, to ensure the security and integrity of the electronic records kept in the system. He also has a system manual to explain to an ATO officer what the system does and how input data is processed by the system in producing the various records and reports.

41. The electronic records kept in the electronic cash book can be audit trailed to original transactions, groups of transactions or summaries of transactions. For instance, the receipts entry in his cashbook for sales made on one particular day can be traced back to a reconciled Z-total on a cash register tape and can be cross-referenced to a reconciled banking deposit entry. The reconciled entry also shows any personal drawings, any cash payments for expenses or stock, etc., for that day.

42. Joe has integrated in the accounting system the use of a simple but convenient computer package that enables him to have better control over his accounts, to know at any point in time his liquidity position and to have a better financial picture of his business.

Example 2

The facts

43. The TC Hotel is an inner suburban pub owned by a husband and wife with an extensive bar trade, restaurant and bistro facilities, a drive-through service, restaurant machines, TAB racing facilities and 30 motel-type accommodation rooms. Its annual turnover currently stands at $7-8 million. Most of its revenue is derived in cash or through credit cards, although recently it has started catering through its restaurant and bistro for local businesses where payment is made by cheque on 30-day account.

44. The hotel has also recently introduced EFTPOS facilities in its restaurant, drive-through bottle shop and gaming areas. A barcode scanner is also in operation in the drive-through as this seems to speed up customer service. All of its cash registers are linked to a central computer facility located in the administration area and every transaction is recorded on a real-time basis, updating relevant ledgers immediately after the transaction occurs. The business purchases all of its supplies on credit and takes full advantage of either the 30- or 60-day terms offered. The hotel employs as many as 30 employees, who are either permanent full-timers or work only on a casual basis.

The system

45. The business’ computer system is fully integrated and revolves around a general ledger. It has the following features:

- it operates on an open item basis, i.e., each transaction is processed immediately after it occurs and triggers the updating of relevant ledgers. For instance, the scanning of a carton of beer in the drive-through department triggers a series of simultaneous transactions. Once the sale is completed either by cash, credit card or through EFTPOS, the inventory records are also immediately updated giving an up-to-the-minute view of the stock level of that particular item;
- each product’s sales can also be called up on screen for viewing, comparison with past months’ sales, etc.;
- reorder points are automatically set in the computer;
- other reports are produced on all aspects of the business’ trading activities including full current bank reconciliation, trial balance at any time, all transaction history and full audit trail;
- the system operates as a network allowing for a number of users to access it at various locations within the hotel at any time. A multi-level password system is employed with some staff only permitted to operate certain functions of the system;
- system support is provided by an elaborate manual, on-screen help functions, demonstration disks and technical support from the software provider; and
- backing-up of the computer files is carried out at the end of each day and the business records are downloaded to floppy disks periodically for the business’ external accountants.
Our view

46. This business’ system, although more sophisticated than the one in the earlier example, is nevertheless subject to tight controls and security safeguards. Access controls are available, as are appropriate audit trails to all transactions that enable the tracing back of any transaction through the system to its origin. The business also has in place a system for backing up its electronic records. Explanations of the system are provided by the manual and other facilities, as well as system support from the software manufacturer. The essential features of each transaction (or batch of transactions) can be explained by the taxpayer on request.

Example 3

The facts

47. Millie Maker (‘MM’) runs a medium-sized printing business. She uses a commercial software accounting package in the business and receives system support from the software manufacturer. MM has retained the software manual that explains the basic aspects of the system she uses.

Issue 1

48. MM has found that storing paper purchase invoices, statements, purchase orders, receipts, etc., is time-consuming and cumbersome. She wishes to explore acceptable alternatives to reduce storage and speed up the retrieval of these records while ensuring that the records are in an acceptable format for ATO purposes.

49. MM has approached Imagery P/L to image her records onto CD-ROMs into a format that is compatible with her current computer system. This will be done once every two months. Original paper records are to be kept prior to being imaged. However, MM proposes to discard the paper records once they are imaged. Her computer system will readily allow her to access and where required, print a hard copy of any of the electronic records. In doing so, an audit trail will automatically be produced to provide details of what actions were taken with that record. MM also proposes to retain an electronic copy of her business’ tax returns, which could be reproduced on paper or electronically on request for a tax officer. She seeks from us our view on her proposal.

Issue 2

50. With the increase in business activity, MM is considering whether to upgrade to a more powerful accounting package from the same software manufacturer or to change over to a new software product. She is particularly interested in knowing what the ATO requirements will be in this latter case as her business records have, for the last five years, been stored under one system.

Our view

Issue 1

51. The ATO would have no difficulty with this proposed system provided the imaged records represent a true and complete copy of the original records. MM would need to confirm that from Imagery P/L. We would also prefer that the imaged records be in ‘read only’ format and for a back-up copy of the records to be stored at a safe location, e.g., at MM’s home. We also accept that once the records have been appropriately imaged, the paper records can be discarded for income tax purposes. During the course of an audit, MM can choose to satisfy our access requests by providing a printed copy of the imaged records sought. However, it may be more practical and less time-consuming for those records to be downloaded onto a disk and made available to us in electronic form.

Issue 2

52. If MM is to simply upgrade, i.e., move from one version of a commercial package to an updated one, there should be no difficulty for the records kept under the old system to be read and accessed under the new system. This is generally provided for in upgrades by software manufacturers. However, she would still need to retain sufficient documentation to explain to us how records under the old system can be recreated under the new system. Generally, the system manual should provide that information. She should check with the software manufacturer on that point.

53. However, should she decide to opt for a new software product, she would need to consider whether to have the records under the old system converted to a form that is acceptable and readable under the new system so that, where necessary, she and an ATO officer can readily access them. Alternatively, she can retain the old records in their current format on some form of electronic storage medium, e.g., CD-ROM, but ensure that there is some mechanism available to have them converted to a form readily readable and retrievable by us. In this case, conversion to a standard data format such as ASCII, DBF or a spreadsheet format would be acceptable. In addition, she would need to retain sufficient information about how the old system operated, the controls (including audit trails) which were in place, and the archiving and backing-up facilities. For commercial packages, this information is generally available in the system manual.

Commissioner of Taxation

5 November 1997

APPENDIX A – CHECKLIST OF ELECTRONIC RECORDS

(The following checklist represents only a guide and should not be taken as an exhaustive list of all records required to explain transactions.)

a) Electronic records (or summary records) of sales transactions such as:
• cash sales, including reconciliations made of cash register tapes;
• credit sales, including electronic copies of merchant statements for sales made by you or alternatively, electronic copies of summary statements of reconciled credit transactions;
• invoices and statements issued, including invoices and statements that you have sent electronically (e.g., via EDI) or imaged copies of hard copy invoices and statements which you have sent;
• credit notes issued for returned goods;
• updates and adjustments to the debtors’ ledger; and
• where appropriate, stock used for private purposes.

b) Electronic records (or summary records) of purchase transactions including:
• cash and credit purchases, including credit card purchases;
• purchase orders issued;
• invoices and statements received from suppliers; these would include invoices and statements that suppliers have sent electronically (e.g., via EDI) to you or imaged copies of hard copy invoices and statements sent to you;
• payment details;
• updates and adjustments to the creditors’ ledger; and
• inventory details, including stocktake lists, price lists details, etc.

c) Electronic records (or summary records) of all other items of income and expenditure such as:
• business expenses like rent, electricity, telephone, insurance, etc.;
• motor vehicle expenses, including records of information kept in car log books and details of odometer readings.

d) Electronic records of quotes provided.

e) Electronic records of information obtained from job sheets.

f) Electronic records (or summary records) of banking transactions including:
• details of deposits;
• details of withdrawals or payments;
• bank statements;
• bank reconciliations; and
• details of any term deposits and any other investments associated with the business.

g) Electronic records of the purchase and disposal of assets; depreciation schedules; etc.

h) Electronic records of all entries to the general ledger and a reconciliation of that ledger to all other subsidiary ledgers.

i) Electronic records of:
• profit and loss statement;
• balance sheet;
• other financial statements;
• schedule of work in progress and raw materials, where applicable, at the end of the financial year; and
• all wages transactions.

j) Audit trails or logs of all electronic transactions including deletions, additions and changes to accounting data.

Previously released in draft form as TR 97/D4
The National Archives and Records Administration Speaks to Electronic Records Retention

The National Archives and Records Administration (NARA) is charged by Congress to preserve the archives and history of the United States. A primary expression of this mission is the collection of permanent records from agencies of the US government for accession to the collection, preservation and retrieval for future researchers. The US government was an early adopter of computer technology; indeed many government and defense initiatives drove much of the nascent computer industry. Early forms of computer output – paper reports – did not pose any new challenges to the archives, as they were well skilled in the collection and preservation of paper. Other early outputs – punched cards and punched tape – while not offering any particular preservation issues, soon pointed up problems with technological obsolescence. Punched cards were in use well into the 1970s, but paper tape soon fell from favor and the hardware and software to read this medium soon disappeared from widespread use. Magnetic tape and disc saw its ascendancy in the 1980s, soon making paper cards and tapes artifacts.

Paper output is still, of course, in common usage, but given the growing volumes of data and information and the complexity of data interdependency in a relational database, preservation on paper becomes highly impractical if not impossible. NARA has for years offered guidelines to agencies on the proper handling of data within the agency and for the transfer of data to the archives.

General Records Schedule 20

This general schedule was first developed in the early 1990s and last revised in 1995; as such, it represents pioneering effort to provide organizational guidelines for the retention of electronic records. Specific only to agencies of the US government and contractors, the schedule does not have authority in the private sector. The schedule does, however, provide a framework and model upon which to approach the management and disposal of common electronic records found in almost any office.

General Records Schedule 24 (proposed)

In May 2002, NARA released for public comment General Records Schedule 24-Information Technology Operations and Management Records. This proposed document has been in review since 1999, and it attempts to schedule “temporary records relating to overall IT management”. As with the GRS 20, the significant value this schedule has for industry is in providing a model for classification of such records routinely found in any IT operation.

Expanding Transfer Options for Electronic Records (proposed)

NARA’s draft expanding the formats it will accept from agencies does not speak directly to record retention per se, but more specifically to media standards and preservation. NARA has proposed the acceptance of Digital Linear Tape for transmittal of records to the archives, if it complies with international standards. File Transfer Protocol is also being advanced as a media-free transfer media, whereby agencies would send data to NARA, again while using accepted file formats.
exist. This schedule has been revised to include electronically generated records previously covered in General Records Schedule 23, Records Common to Most Offices. The original numbering of the items in GRS 20 has been preserved. The items moved from GRS 23 have been added at the end, except the item covering administrative databases that has been incorporated into item 3.

Electronic versions of records authorized for disposal elsewhere in the GRS may be deleted under the provisions of item 3 of GRS 20. See also 36 CFR Part 1234 for NARA regulations on electronic records management.


a. Electronic files or records created solely to test system performance, as well as hard-copy printouts and related documentation for the electronic files/records.

Delete/destroy when the agency determines that they are no longer needed for administrative, legal, audit, or other operational purposes.

b. Electronic files or records used to create or update a master file, including, but not limited to, work files, valid transaction files, and intermediate input/output records.

Delete after information has been transferred to the master file and verified.

c. Electronic files and hard-copy printouts created to monitor system usage, including, but not limited to, log-in files, password files, audit trail files, system usage files, and cost-back files used to assess charges for system use.

Delete/destroy when the agency determines they are no longer needed for administrative, legal, audit, or other operational purposes.

2. Input/Source Records.

a. Nonelectronic documents or forms designed and used solely to create, update, or modify the records in an electronic medium and not required for audit or legal purposes (such as need for signatures) and not previously scheduled for permanent retention in a NARA-approved agency records schedule.

Destroy after the information has been converted to an electronic medium and verified, or when no longer needed to support the reconstruction of, or serve as the backup to, the master file, whichever is later.

b. Electronic records, except as noted in item 2c, entered into the system during an update process, and not required for audit and legal purposes.

Delete when data have been entered into the master file or database and verified, or when no longer required to support reconstruction of, or serve as backup to, a master file or database, whichever is later.

c. Electronic records received from another agency and used as input/source records by the receiving agency, EXCLUDING records produced by another agency under the terms of an interagency agreement, or records created by another agency in response to the specific information needs of the receiving agency.

Delete when data have been entered into the master file or database and verified, or when no longer needed to support reconstruction of, or serve as backup to, the master file or database, whichever is later.

d. Computer files or records containing uncalibrated and unvalidated digital or analog data collected during observation or measurement activities or research and development programs and used as input for a digital master file or database.

Delete after the necessary data have been incorporated into a master file.


a. Electronic versions of records that are scheduled for disposal under one or more items in GRS 1-16, 18, 22, or 23; EXCLUDING those that replace or duplicate the following GRS items: GRS 1, items 21, 22, 25f; GRS 12, item 3; and GRS 18, item 5.

Delete after the expiration of the retention period authorized by the GRS or when no longer needed, whichever is later.

b. Electronic records that support administrative housekeeping functions when the records are derived from or replace hard copy records authorized by NARA for destruction in an agency-specific records schedule.

(1) When hard copy records are retained to meet recordkeeping requirements.

Delete electronic version when the agency determines that it is no longer needed for administrative, legal, audit, or other operational purposes.

(2) When the electronic record replaces hard copy records that support administrative housekeeping functions.

Delete after the expiration of the retention period authorized for the hard copy file, or when no longer needed, whichever is later.

(3) Hard copy printouts created for short-term administrative purposes.

Delete when the agency determines that they are no longer needed for administrative, legal, audit, or other operational purposes.

4. Data Files Consisting of Summarized Information.

Records that contain summarized or aggregated information created by combining data elements or individual
observations from a single master file or database that is disposable under a GRS item or is authorized for deletion by a disposition job approved by NARA after January 1, 1988, EXCLUDING data files that are created as disclosure-free files to allow public access to the data which may not be destroyed before securing NARA approval.

Delete when the agency determines that they are no longer needed for administrative, legal, audit, or other operational purposes.

[NOTE: Data files consisting of summarized information which were created from a master file or database that is unscheduled, or that was scheduled as permanent but no longer exists or can no longer be accessed, may not be destroyed before securing NARA approval.]

5. Records Consisting of Extracted Information.

Electronic files consisting solely of records extracted from a single master file or database that is disposable under GRS 20 or approved for deletion by a NARA-approved disposition schedule, EXCLUDING extracts that are:

a. produced as disclosure-free files to allow public access to the data; or

b. produced by an extraction process which changes the informational content of the source master file or database, which may not be destroyed before securing NARA approval. For print and technical reformat files see items 6 and 7 of this schedule respectively.

Delete when the agency determines that they are no longer needed for administrative, legal, audit, or other operational purposes.

[NOTES: (1) Records consisting of extracted information that was created from a master file or database that is unscheduled, or that was scheduled as permanent but no longer exists or can no longer be accessed may not be destroyed before securing NARA approval. (2) See item 12 of this schedule for other extracted data.]

6. Print File.

Electronic file extracted from a master file or database without changing it and used solely to produce hard-copy publications and/or printouts of tabulations, ledgers, registers, and statistical reports.

Delete when the agency determines that they are no longer needed for administrative, legal, audit, or other operational purposes.


Electronic file consisting of data copied from a complete or partial master file or database made for the specific purpose of information interchange and written with varying technical specifications, EXCLUDING files created for transfer to the National Archives.

Delete when the agency determines that they are no longer needed for administrative, legal, audit, or other operational purposes.

8. Backups of Files.

Electronic copy, considered by the agency to be a Federal record, of the master copy of an electronic record or file and retained in case the master file or database is damaged or inadvertently erased.

a. File identical to records scheduled for transfer to the National Archives.

Delete when the identical records have been captured in a subsequent back-up file or when the identical records have been transferred to the National Archives and successfully copied.

b. File identical to records authorized for disposal in a NARA-approved records schedule.

Delete when the identical records have been deleted, or when replaced by a subsequent back-up file.


Electronic indexes, lists, registers, and other finding aids used only to provide access to records authorized for destruction by the GRS or a NARA-approved SF 115, EXCLUDING records containing abstracts or other information that can be used as an information source apart from the related records.

Delete with related records or when the agency determines that they are no longer needed for administrative, legal, audit, or other operational purposes, whichever is later.

10. Special Purpose Programs.

Application software necessary solely to use or maintain a master file or database authorized for disposal in a GRS item or a NARA-approved records schedule, EXCLUDING special purpose software necessary to use or maintain any unscheduled master file or database or any master file or database scheduled for transfer to the National Archives.

Delete when related master file or database has been deleted.

11. Documentation.

a. Data systems specifications, file specifications, codebooks, record layouts, user guides, output specifications, and final reports (regardless of medium) relating to a master file or database that has been authorized for destruction by the GRS or a NARA-approved disposition schedule.

Destroy or delete when superseded or obsolete, or upon authorized deletion of the related master file or database, or upon the destruction of the output of the system if the output is needed to protect legal rights, whichever is latest.
b. Copies of records relating to system security, including records documenting periodic audits or review and recertification of sensitive applications, disaster and continuity plans, and risk analysis, as described in OMB Circular No. A-130.

Destroy or delete when superseded or obsolete.

[NOTES: (1) Documentation that relates to permanent or unscheduled master files and databases is not authorized for destruction by the GRS. (2) See item 1a of this schedule for documentation relating to system testing.]

12. Downloaded and Copied Data.

Derived data and data files that are copied, extracted, merged, and/or calculated from other data generated within the agency, when the original data is retained.

a. Derived data used for ad hoc or one-time inspection, analysis or review, if the derived data is not needed to support the results of the inspection, analysis or review.

Delete when the agency determines that they are no longer needed for administrative, legal, audit, or other operational purposes.

b. Derived data that provide user access in lieu of hard-copy reports that are authorized for disposal.

Delete when the agency determines that they are no longer needed for administrative, legal, audit, or other operational purposes.

c. Metadata or reference data, such as format, range, or domain specifications, which is transferred from a host computer or server to another computer for input, updating, or transaction processing operations.

Delete from the receiving system or device when no longer needed for processing.

[NOTE: See item 5 of this schedule for other extracted data.]


Documents such as letters, memoranda, reports, handbooks, directives, and manuals recorded on electronic media such as hard disks or floppy diskettes after they have been copied to an electronic recordkeeping system, paper, or microform for recordkeeping purposes.

Delete from the word processing system when no longer needed for updating or revision.


Senders’ and recipients’ versions of electronic mail messages that meet the definition of Federal records, and any attachments to the record messages after they have been copied to an electronic recordkeeping system, paper, or microform for recordkeeping purposes.

Delete from the e-mail system after copying to a recordkeeping system.

[NOTE: Along with the message text, the recordkeeping system must capture the names of sender and recipients and date (transmission data for recordkeeping purposes) and any receipt data when required.]

15. Electronic Spreadsheets.

Electronic spreadsheets generated to support administrative functions or generated by an individual as background materials or feeder reports.

a. When used to produce hard copy that is maintained in organized files.

Delete when no longer needed to update or produce hard copy.

b. When maintained only in electronic form.

Delete after the expiration of the retention period authorized for the hard copy by the GRS or a NARA-approved SF 115. If the electronic version replaces hard-copy records with differing retention periods and agency software does not readily permit selective deletion, delete after the longest retention period has expired.
Request for Comments RIN 3095-ZA04
AGENCY: National Archives and Records Administration.
ACTION: Notice of proposed records schedule; request for comments.
SUMMARY: As required by statute (44 U.S.C. 3303a(d)), the National Archives and Records Administration (NARA) issues General Records Schedules (GRS) to provide disposal authority for temporary administrative records common to several or all agencies of the Federal Government. The GRS include records relating to civilian personnel, fiscal accounting, procurement, communications, printing, and other common functions. NARA has developed a new General Records Schedule, Information Technology Operations and Management Records, to provide disposal authority for certain administrative records generated in or acquired by agency components responsible for developing and operating network infrastructure and systems.
NARA invites public comments on this proposed new general records schedule, as required by 44 U.S.C. 3303a(a). Because of the widespread interest in the management of electronic records, NARA is publishing the full text of the schedule with additional information on each item.
DATES: Comments must be received in writing on or before August 26, 2002.
ADDRESSES: Comments should be sent to Modern Records Programs (NWM), National Archives at College Park, 8601 Adelphi Road, College Park, MD 20740-6001, faxed to 301-837-3697 or 301-837-3698, or sent to the following Internet address: records.mgt@nara.gov.
FOR FURTHER INFORMATION CONTACT: Michael L. Miller, Director, Modern Records Programs, 301-837-1980.
SUPPLEMENTARY INFORMATION: In 1978, use of the GRS was made legally mandatory. A Federal agency must destroy records in accordance with the GRS to the greatest extent possible. If an agency wishes to apply a different retention period for any series of records included in the GRS, the records officer must submit a Standard Form (SF) 115 providing justification for the desired deviation.
Relationship of This Draft GRS to GRS 20, Electronic Records
This schedule does not duplicate or replace GRS 20, Electronic Records. The proposed new schedule addresses the administrative records generated by units responsible for technical management of IT resources. The functions covered by the proposed GRS 24 are comparable to the administrative functions relating to budgeting, contracting, human resources, and property management that are covered by other GRS. The proposed GRS 24 does not apply to system data or information content, which must be scheduled separately by submitting an SF 115, Request for Records Disposition Authority, to NARA.
GRS 20 remains in effect to cover the records described in that schedule. GRS 20 records include certain files associated with temporary database management systems such as print files, extract files, source records, and certain disposable electronic records produced by end-users in office automation applications. NARA will conduct a separate review concerning the continuation of GRS 20 disposition authorities as part of its comprehensive review of the policies and procedures for scheduling and appraisal of records in all formats.
Background—Development of This Draft GRS
In late 1997, the Archivist established an interagency Electronic Records Work Group to review General Records Schedule 20 and recommend revisions to that schedule or other practical solutions for the scheduling of electronic records. In 1998, the work group submitted its final report to the Archivist (http://www.archives.gov/records_management/policy_and_guidance/report_to_archivist_0998.html) recommending, among other things, that NARA issue a new general records schedule for information technology operations and management records to supplement, not replace, GRS 20.
Building on the efforts of the Work Group, NARA drafted a new GRS for common administrative records relating to operation and management of information technology and related services. Federal agencies reviewed the draft in the summer of 1999. The draft, revised in response to agency comments, was discussed at a January 2000 focus group meeting with agency records management and information technology management officials. NARA made appropriate changes in response to comments made at the meeting and in June 2000 again requested comments from Federal agencies.
Overall, agencies found that the schedule draft they reviewed in 2000 generally fits their records and could be implemented without undue difficulty. In response to specific comments about terminology, apparent redundancies, and retention periods for some items, NARA consolidated some items and provided other clarifications to address the concerns. NARA believes the schedule is now at the appropriate level of detail. Given the agencies’ interest in having more flexibility in applying disposition standards for temporary records, NARA eliminated the cutoff instructions and reworded some of the disposition instructions to allow agencies disposition options based on their internal procedures and operations. NARA clarified that the schedule covers only the temporary adminis-
appendix - General Records Schedule 24

Introduction
This schedule provides disposal authorization for certain files created and maintained in the operation and management of information technology (IT) and related services. As defined in the Information Technology Management Reform Act of 1996 (now the Clinger-Cohen Act), “information technology” includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.

This GRS does not cover all records relating to information technology operations and management. Offices with responsibility for IT operations also maintain administrative records covered by other GRS and records not in the GRS that must be scheduled by the agency. In addition, this GRS does not apply to system data or information content, which must be scheduled separately by submitting an SF 115, Request for Records Disposition Authority, to NARA.

The disposition instructions apply to records regardless of physical form or characteristics. Records may be maintained on paper, in microform, or electronically. Dispositions apply, however, only to records that are maintained as described in each item or subitem. If documents are part of a larger case file or recordkeeping system that contains records not covered in this GRS, agencies must separately schedule that file or system by submitting an SF 115 to NARA. If records covered by more than one item in this schedule are maintained together in one file or recordkeeping system, agencies must retain the records for the longest retention period authorized for those items.

Note that GRS 20, Electronic Records, remains in effect. GRS 20 covers certain temporary files associated with database management. This new schedule supplements GRS 20 by providing disposal authority for temporary records relating to overall IT management, as opposed to the operation and use of specific systems. NARA is reviewing alternatives to GRS 20 and will develop revised requirements as it explores new approaches to managing electronic records.

1. Oversight and Compliance Files
Records in offices with agency-wide or bureau-wide responsibility for managing IT operations relating to compliance with IT policies, directives, and plans including recurring and special reports, responses to findings and recommendations, and reports of follow-up activities.

a. Performance measurements and benchmarks.
Destroy/delete when 5 years old or 1 year after responsible office determines that there are no unresolved issues, whichever is longer.

b. All other oversight and compliance records including:
Certification and accreditation of equipment
Quality assurance reviews and reports
Reports on implementation of plans
Compliance reviews
Data measuring or estimating impact and compliance
Destroy/delete when 3 years old or 1 year after responsible office determines that there are no unresolved issues, whichever is longer.

[Note: See item 3b for performance files relating to systems.]

[Appraisal analysis: Item 1a covers such records as statistical performance data concerning system (and network) operations, including process steps or paths, time required for completion, and event or error indicators. These records include system availability reports that draw upon sample performance indicators to measure overall system performance. The retention period for this item relates to the “5 year plans” typically associated with IT systems.

Item 1b covers such materials as target IT architecture reports, systems development lifecycle handbooks, computer network assessments and follow-up documenta-
tion, authority to operate records, and certification and accreditation of equipment. These records are critical to the proper functioning of systems. Network assessments, for example, are conducted at regular intervals, and in cases where performance is found to be in need of improvement, the agency institutes a process to change or upgrade network equipment, configuration, or other components. Records under this item typically take the form of structured reports. Examples include contractor evaluation reports and other quality assurance records, market analyses and performance surveys, and benefit-cost analyses. Agencies may also maintain other compliance reviews including related analyses such as histograms illustrating trends across time for various groups, activities, and systems, and follow-up correspondence and corrective action reports.

The proposed dispositions for these will ensure the availability of records for a period of time that is sufficient to allow adequate systems management and will also ensure the preservation of records identifying problems until the problems have been resolved.[2]

2. IT Facility, Site Management, and Equipment Support Services Records.

Records maintained by offices responsible for the control and operation of buildings and rooms where IT equipment, systems, and storage media are located including:

- Files identifying IT facilities and sites, and
- Files concerning implementation of IT facility and site management and equipment support services provided to specific sites, including reviews, site visit reports, trouble reports, equipment service histories, reports of follow-up actions, and related correspondence.

Destroy/delete when 3 years old, or when superseded or obsolete, whichever is longer.

[Appraisal analysis: These records document the control and operation of buildings and rooms where IT equipment, systems, and storage media are located. Files include listings of facilities, trouble reports, reports on site visits and inspections, and service histories for equipment. Also included are copies of agency directives and lines of authority relating to such matters as facility operations, physical security of facilities, environmental security, including documents on fire prevention and control, electric power supply protection, magnetism protection, and “good housekeeping” procedures for protection against dust, dirt, and fire hazards.

These records need only to be kept for a relatively short period of time to satisfy administrative and operational needs. The proposed three-year retention period is adequate to ensure that IT operations are carried out in an environment that meets all applicable standards.

Records documenting control and operation of facilities that are maintained by units responsible for facilities management and physical security are retained for varying periods of time in accordance with other GRS items (e.g., GRS 18, items 9 and 10) and individual agency schedules.]

3. IT Asset and Configuration Management Files.

- a. Inventories of IT assets, network circuits, and building or circuitry diagrams, including equipment control systems such as databases of barcodes affixed to IT physical assets. Destroy/delete 1 year after completion of the next inventory.
- b. Records created and retained for asset management, performance and capacity management, system management, configuration and change management, and planning, follow-up, and impact assessment of operational networks and systems. Includes, but is not limited to:
  1. Data and detailed reports on implementation of systems, applications and modifications; application sizing, resource and demand management; documents identifying, requesting, and analyzing possible changes, authorizing changes, and documenting implementation of changes; documentation of software distribution and release or version management.

Destroy/delete 1 year after termination of system.

(2) Records of IT maintenance on the network infrastructure documenting preventative, corrective, adaptive and perfective (enhancement) maintenance actions, including requests for service, work orders, service histories, and related records.

Destroy/delete when 3 years old or 1 year after termination of system, whichever is sooner.

[Appraisal analysis: This item covers routine administrative records relating to existing IT systems, such as inventories of assets, including equipment control systems, databases of barcodes affixed to physical assets, work orders and service histories on maintenance of network infrastructure, and reports and other files relating to system implementation and modification. Detailed information is found in bar code reports, asset management guides, requests for services, requisitions for equipment, leases, change orders, purchase orders, property transfer control systems, flow configuration requests, standardization requests and justifications. Other records include listings of devices such as routers, hubs, switches, and servers, described by make and model, location, and pertinent capacity and configuration information. These records differ from those covered by item 11. The records under item 3 relate to the ongoing maintenance and management of existing IT assets. The records under item 11 relate to the acquisition and implementation of new systems.

The proposed retention period in item 3a is appropriate since only current inventories are needed. Note that documents (or sections of documents) that are unchanged from prior inventories but that remain valid are kept in conjunction with current inventories. The proposed disposition instructions for item 3b(1) reflects the business need to retain for the life of a system detailed reports and data concerning the implementation, modification, and upgrading of systems infrastructure. For item 3b(2), the proposed disposition enables disposal of system maintenance records when three years old or one year after termination of the system, whichever is sooner. This will enable the agencies to ensure that proper maintenance
procedures have been followed and to allow for any follow-up activities. If any maintenance activities have a major impact on a system, or lead to a significant change, those activities should be documented in item 3b(1).]


a. Backup tapes maintained for potential system restoration in the event of a system failure or other unintentional loss of data.

(1) Delete/destroy incremental back-up tapes when superseded by a full backup, or when no longer needed for system restoration, whichever is later.

(2) Delete/destroy full back-up tapes when second subsequent backup is verified as successful or when no longer needed for system restoration, whichever is later.

[Note: See GRS 20, item 8, for backups of master files and databases.] Delete/destroy when superseded or obsolete.

[Appraisal analysis: This item pertains to records accumulated to ensure the ability to resume operations in the event of a system failure. Item 4a covers incremental and full system back-up tapes maintained for potential system restoration. It is distinguished from GRS 20, item 8, Backups of Files, which covers security copies of the substantive contents of master files and databases. The GRS 24 item applies to an IT shop’s backups of system software (which, due to system configuration, may also include substantive data separately covered under GRS 20, item 8). Item 4b applies to Tape Library records including automated files and manual records used to control the location, maintenance, and disposition of magnetic media in a tape library including list of holdings and control logs. Delete/destroy when superseded or obsolete.

b. Tape library records including automated files and manual records used to control the location, maintenance, and disposition of magnetic media in a tape library providing records used to control the location, maintenance, and disposition of magnetic media in a tape library provides for destruction when they are superseded, obsolete, or no longer needed. This authorization is appropriate because agencies need only the current, accurate information on the location and status of back-up tapes.]

5. Files Related to Maintaining the Security of Systems and Data.


Destroy/delete 1 year after system is superseded.

b. Documents identifying IT risks and analyzing their impact, risk measurements and assessments, actions to mitigate risks, implementation of risk action plan, service test plans, test files and data.

Destroy/delete 1 year after system is superseded.

[Appraisal analysis: Item 5a provides disposal authority for records that outline official procedures for securing and maintaining IT infrastructure, typically system security plans, disaster recovery plans, and continuity of operations plans. The files include such records as published computer technical manuals and guides, examples and references used to produce guidelines covering security issues related to specific systems and equipment, records on disaster exercises and resulting evaluations, network vulnerability assessments, risk surveys, and other studies, such as formal security vulnerability assessments conducted by IG offices. These records relate to the specific systems for which they were written. System replacements will have new security and risk management requirements that may be totally different because of the architecture of the replacement system. The disposition instruction for item 5a provides for maintenance of the records to ensure a continuity of security controls throughout the life of the system.

Item 5b covers analysis of security policies, processes, and guidelines, as well as system risk management and vulnerability analyses. Examples of specific documents are automated information systems security directives and computer virus handbooks. Records covered by GRS 18, item 27 may appear similar, but GRS 18 relates to plans developed to protect life and property and GRS 24 covers records relating specifically to the security of IT systems. The retention period for these records reflects the need to retain records while a system is current and provides for review of documentation for superseded systems in connection with ensuring adequate protection for new systems.]

6. User Identification, Profiles, Authorizations, and Password Files EXCLUDES records relating to electronic signatures.

a. Systems requiring special accountability, e.g., those containing information that may be needed for audit or investigative purposes and those that contain classified records.

Destroy/delete inactive file 6 years after user account is terminated or password is altered, or when no longer needed for investigative or security purposes, whichever is later.
b. Routine systems, i.e., those not covered by item 6a. See GRS 20, item 1c.

[Appraisal analysis: Item 6a provides disposition instructions for user identification records, including user profiles and passwords associated with systems requiring special accountability, such as systems containing information that is security classified. The item authorizes the destruction of records concerning user identification six years after a user account is terminated or password is altered, or when it is no longer needed for security purposes, whichever is later. This will permit agencies to retain user identification records associated with highly sensitive or potentially vulnerable systems in order to provide historical data that may be needed in support of investigations or litigation arising from inappropriate access.

Records covered under item 6b include records such as user passwords and profiles for those systems not requiring special accountability. The records in these systems are typically system generated according to preset requirements. A system may, for example, prompt users for new passwords every 90 days for all users. These records are covered by GRS 20, Item 1c.]

7. Computer Security Incident Handling, Reporting and Follow-up Records

Destroy/delete 3 years after all necessary follow-up actions have been completed.

[Appraisal analysis: This item covers records relating to attempted or actual system security breaches, including break-ins (“hacks”), virus threats, improper staff usage, failure of security provisions or procedures, and potentially compromised information assets.

These records typically consist of narrative reports and background documentation relating to individual events or issues. These records include references to unauthorized intrusions, web site defacement, misuse of system resources, and other incidents noted by the Federal Computer Incident Response Center (FedCIRC, http://www.fedcirc.gov/).

Retaining records for 3 years after all follow-up actions, including judicial procedures, have been completed ensures the availability of active case records and provides an adequate amount of time after a case is closed for any necessary follow-up action. Any significant incidents (e.g., a major system failure or compromise of critical government data) would be documented in program records, such as those in the office of the Inspector General, which must be scheduled separately by submitting an SF 115 to NARA.]

8. IT Operations Records

a. Workload schedules, run reports, and schedules of maintenance and support activities.

Destroy/delete when 1 year old.

b. Problem reports, proposals for changes and related decision documents relating to the software infrastructure of the network or system.

Destroy/delete 1 year after problem is resolved.

c. Reports on operations, including measures of benchmarks, performance indicators, and critical success factors, error and exception reporting, self-assessments, performance monitoring, and management reports.

[Appraisal analysis: Item 8a includes workload schedules, run reports, including cycle time reports, schedules of maintenance, and related records. It is generally agreed within the Federal IT community that the value of these voluminous records expires after one year.

Item 8b covers problem reports, proposals for changes and related decision documents relating to the software infrastructure of a network or system. The retention period proposed for these records will satisfy the administrative and operational needs of IT offices by ensuring the retention of records related to issues until they have been resolved.

Item 8c covers reports on operations, including measures of benchmarks, performance monitoring, and management reports. Agencies indicated that the proposed retention period would meet their administrative and operational requirements for these routine files.]

9. Financing of IT Resources and Services

[Note: Copies of records needed to support contracts should be filed in procurement files, which are scheduled under GRS 3.]

a. Agreements formalizing performance criteria for quantity and quality of service, including definition of responsibilities, response times and volumes, charging, integrity guarantees, and nondisclosure agreements. Destroy/delete 3 years after agreement is superseded or terminated.

b. Files related to managing third-party services, including records that document control measures for reviewing and monitoring contracts and procedures for determining their effectiveness and compliance. Destroy/delete 3 years after control measures or procedures are superseded or terminated.

c. Records generated in IT management and service operations to identify and allocate charges and track payments for computer usage, data processing and other IT services EXCLUDING records that are part of the agency’s cost accounting system, which are covered in GRS 8, items 6 and 7.

Destroy/delete records with no outstanding payment issues when 3 years old.

[Appraisal analysis: These records include agreements formalizing performance criteria for quantity and quality of service, files related to managing third-party services, and records generated in IT management and service operations, financial records including service level agreements defining service and support levels in quantified terms workload, hardware, software, as well as ad hoc reports documenting the continued validity of financial agreements. Records also include documentation related to contractor award fee for superior service.

These records relate to financial management, not IT equipment and services per se, and should be kept for
three years after agreements, procedures, and payment issues are superseded, terminated, or resolved, as applicable. This retention period reflects normal audit cycles. These files are kept by IT offices to support their role in the acquisition of and payment for computer software and services. Records pertaining to these subjects that are needed to protect legal rights, address fiscal concerns, and/or provide Government accountability are maintained in procurement and finance offices in accordance with other GRS items or agency schedules.]

10. IT Customer Service Files
   a. Records related to providing help desk information to customers, including pamphlets, responses to “Frequently Asked Questions,” and other documents prepared in advance to assist customers. Destroy/delete after record is superseded or obsolete.
   b. Help desk logs and reports and other files related to customer query and problem response; query monitoring and clearance; and customer feedback records; and related trend analysis and reporting. Destroy/delete when 1 year old or when no longer needed for review and analysis, whichever is later.

   [Appraisal analysis: The records covered by Item 10 relate to providing customer service and individual support to customers. Included are such records as pamphlets and Frequently Asked Questions, help desk logs and incident reports, “help desk tickets,” user guides, trouble reports, customer queries, feedback records, and trend analyses. These document end-user inquiries and requests for assistance.
   These voluminous records are critical to the effective operation of IT systems. However, they have administrative value for only a brief period of time. This item will authorize destruction of customer service records such as pamphlets and lists of “frequently asked questions” (FAQs) one year after the record is superseded or obsolete and that help desk logs and other files related to customer query, feedback, and analysis be destroyed when one year old. The recommended disposition instructions will satisfy the administrative and operational needs of IT offices, including the need to dispose of these files in a timely fashion.]

11. IT Infrastructure Design and Implementation Files
   Records of individual projects designed to provide and support new agency IT infrastructure (see Note), systems, and services. Includes records documenting:
   --Requirements for and implementation of functions such as --Maintaining network servers, desktop computers, and other hardware --Installing and upgrading network operating systems and shared applications --Providing data telecommunications
   Infrastructure development and maintenance such as --Acceptance/accreditation of infrastructure components --Analysis of component options, feasibility, costs and benefits --Work associated with implementation, modification, and troubleshooting
   --Models, diagrams, schematics, and technical documentation
   --Quality assurance reviews and test plans, data, and results.
   a. Records for projects that are not implemented. Destroy/delete 1 year after final decision is made.
   b. Records for projects that are implemented. Destroy/delete 5 years after project is terminated.
   c. Installation and testing records. Destroy/delete 3 years after final decision on acceptance is made.

   [Note: IT Infrastructure means the basic systems and services used to supply the agency and its staff with access to computers and data telecommunications. Components include hardware such as printers, desktop computers, network and web servers, routers, hubs, and network cabling, as well as software such as operating systems (e.g., Microsoft Windows and Novell NetWare) and shared applications (e.g., electronic mail, word processing, and database programs). The services necessary to design, implement, test, validate, and maintain such components are also considered part of an agency’s IT infrastructure. However, records relating to specific systems that support or document mission goals are not covered by this item and must be scheduled individually by the agency by submission of an SF 115 to NARA.]

   [Appraisal analysis: These records pertain to individual new enterprise projects designed to provide and support agency IT infrastructure. IT infrastructure includes the basic systems and services used to supply the agency and its staff with access to computers and data telecommunications. Included are hardware, software, and the services necessary to design, implement, and maintain such components. This item covers records concerning the infrastructure of IT operations. These records do not document programs fundamental to an agency’s mission nor the IT systems utilized by agencies in carrying out their distinctive functions. Rather, these records are clearly administrative in nature and are of the same character throughout the Government. Records include developmental records such as quality assurance plans, requirement specifications, technology refresh plans, operational support and test plans, final operational support plan, and post installation reviews and briefings. These records differ from those found in Item 3 above. Item 3 is concerned with the ongoing maintenance and management of existing IT assets. Item 11 is concerned with the acquisition and implementation of new operating systems.
   The disposition instruction for item 11a provides that records for projects that are not implemented be destroyed/deleted one year after a final decision has been made. This retention period is appropriate. If a proposed project is rejected, there is no need to retain the related records for an extended period of time. In accordance with Item 11b, records for projects that are implemented are to be destroyed five years after the project terminates. This proposed retention period will ensure that records germane to a requirement are available while the requirement
is still current and for a period of time thereafter for use in developing new projects. In item 11c, installation and testing records are proposed for destruction or deletion 3 years after the final decision on acceptance is made. This retention period will ensure the availability of records should problems develop and is also consistent with audit cycles.

12. Electronic Mail and Word Processing System Copies

Electronic copies of records that are created on electronic mail and word processing systems and used solely to generate a recordkeeping copy of the records covered by the other items in this schedule. Also includes electronic copies of records created on electronic mail and word processing systems that are maintained for updating, revision, or dissemination.

a. Copies that have no further administrative value after the recordkeeping copy is made. Includes copies maintained by individuals in personal files, personal electronic mail directories, or other personal directories on hard disk or network drives, and copies on shared network drives that are used only to produce the recordkeeping copy. Destroy/delete within 180 days after the recordkeeping copy has been produced.

b. Copies used for dissemination, revision, or updating that are maintained in addition to the recordkeeping copy. Destroy/delete when dissemination, revision, or updating is completed.

[Appraisal analysis: This item will provide disposal authority for electronic mail (email) and word processing records used solely to produce records described in GRS 24, after a recordkeeping copy has been produced, and electronic copies of records described in GRS 24 used solely for dissemination, revision, or updating that are maintained in addition to the recordkeeping copy. In 1998 NARA added an item with the same wording as this item 12 to GRS 1-16, 18, and 23. Item 12 is in keeping with the authority that exists throughout the GRS to dispose of email and word processing copies of records within the scope of each GRS. Agencies should use agency specific schedules developed following the guidance in NARA Bulletin 2001-03 or GRS 20 Items 13 and 14 to dispose of email and word processing copies of other information technology records (i.e., records not covered by this GRS) that are not required for recordkeeping purposes. Please note that neither this item in GRS 24, the identical items in other GRS, nor GRS 20, items 13 and 14, apply to the copies of email and word processing records that are designated for recordkeeping purposes.]


Michael J. Kurtz,
Assistant Archivist for Records Services—Washington DC.
SUMMARY: This proposed rule will amend the regulations for the transfer of permanent records to NARA by permitting two additional electronic records transfer methods, File Transfer Protocol (FTP) and Digital Linear Tape IV (DLT tape IV). NARA is introducing these transfer methods to reduce the media and shipping costs of electronic records transferred from Government agencies, improve record and file integrity, and expand the options for transfer methods. This rule will affect Government agencies transferring permanent electronic records to the National Archives of the United States.

DATES: Comments are due by August 26, 2002.

ADDRESSES: Comments must be sent to Regulation Comment Desk (NPOL), Room 4100, Policy and Communications Staff, National Archives and Records Administration, 8601 Adelphi Road, College Park, MD 20740-6001. They may be faxed to 301-837-0319. You may also comment via the Internet to comments@nara.gov.

FOR FURTHER INFORMATION CONTACT: Jennifer Davis Heaps at telephone number 301-837-1801, or fax number 301-837-0319.

SUPPLEMENTARY INFORMATION: NARA currently accepts magnetic tape and compact-disk, read only memory (CD-ROM) as transfer media for records scheduled for permanent retention in the National Archives of the United States. DLT tape IV is a kind of magnetic tape cartridge. NARA has used only media-based transfer methods in the past, but has been testing other methods as well as additional media. With this rule, NARA proposes the addition of FTP transfer methods and DLT transfer media. FTP is a media-less transfer method that can be used to transfer electronic records. FTP operates by using special software located at the sending and receiving sites. This software, in combination with a telecommunications network, provides the means for transferring electronic records. The agency may send any documentation in electronic format to NARA via FTP as part of the transfer of the electronic records or through any other accept-

able method of transfer as specified in 36 CFR 1228.270. DLT tape IV cartridge tape is a high-density magnetic cartridge tape that can store up to 40 gigabytes of information on each cartridge. DLT tape IV tapes are used by selected tape drive units produced by several companies. DLT tape IV preparation will follow existing cartridge tape specifications. Paragraphs (a) and (b) in Sec. 1228.270 have been rewritten for clarity and consistency with the new information in paragraph (c) of the same section.

Although this proposed rule does not address the format of electronic records described in paragraph (d), NARA is exploring the acceptance of formats other than ASCII and EBCDIC as part of its E-Government initiative. Any proposed changes in this area will be addressed in a separate rulemaking.

Please submit Internet comments within the body of your email message or as an attachment. Please also include “Attn: 3095-AB03” and your name and return address in your Internet message. If you do not receive a confirmation from the system that we have received your Internet message, contact the Regulation Comment Desk at 301-837-1801.

This proposed rule is a significant regulatory action for the purposes of Executive Order 12866 and has been reviewed by the Office of Management and Budget. As required by the Regulatory Flexibility Act, I certify that this rule will not have a significant impact on a substantial number of small entities because it applies only to Federal agencies.

This regulation does not have any federalism implications.

List of Subjects in 36 CFR Part 1228 Archives and records.

For the reasons set forth in the preamble, NARA proposes to amend part 1228 of title 36, Code of Federal Regulations, as follows:

PART 1228—DISPOSITION OF FEDERAL RECORDS

1. The authority citation for part 1228 continues to read as follows:

Authority: 44 U.S.C. chs. 21, 29, and 33.

2. Amend Sec. 1228.270 by revising paragraphs (a), (b), and (c) to read as follows:

Sec. 1228.270 Electronic records.

(a) Timing of transfers. Each agency is responsible for the integrity of the permanent records it transfers on physical media to the National Archives of the United States. For records transferred by a media-less method, NARA works with the agency to ensure integrity of the records during the transfer process. To ensure that permanent electronic records are preserved, each Federal agency must transfer electronic records to NARA promptly in accordance with the agency's records disposition schedule. Furthermore, if the agency cannot provide proper care and handling of the media (see part 1234 of this chapter), or if the media are becoming obsolete and the agency cannot migrate the records to newer media, the agency must contact NARA to
arrange for timely transfer of permanent electronic records, even when sooner than provided in the records schedule.

(b) Temporary retention of copy. Each agency must retain a second copy of any permanent electronic records that it transfers to the National Archives of the United States until it receives official notification from NARA that the transfer was successful and that NARA has assumed responsibility for continuing preservation of the records.

(c) Transfer media. This paragraph covers the transfer of permanent records to the National Archives; it does not apply to the use or storage of records in agency custody. See 36 CFR 1234.30 for the requirements governing the selection of electronic records storage media for current agency use. The agency must use only media that is sound and free from defects for transfers to the National Archives of the United States; the agency must choose reasonable steps to meet this requirement. The approved media and media-less transfer forms are open-reel magnetic tape, magnetic tape cartridge; Compact-Disk, Read Only Memory (CD-ROM); and File Transfer Protocol (FTP) as described in paragraphs (c) (1), (2) and (3) of this section.

(1) Magnetic tape. Agencies may transfer electronic records to the National Archives on magnetic tape as follows:

(i) Open-reel magnetic tape must be on \( \frac{1}{2} \) inch 9-track tape reels recorded at 1600 or 6250 bpi that meet ANSI X3.39-1986, American National Standard: Recorded Magnetic Tape for Information Interchange (1600 CPI, PE) or ANSI X3.54-1986, American National Standard: Recorded Magnetic Tape for Information Interchange (6250 CPI, Group Coded Recording), respectively.

(ii) Tape cartridges may be 18-track 3480-class cartridges. The 3480-class cartridge must be recorded at 37,871 bpi that meet ANSI X3.180-1990, American National Standard: Magnetic Tape and Cartridge for Information Interchange—18-Track, Parallel, \( \frac{1}{2} \) inch (12.65 mm), 37871 cpi (1491 cpm), Group Coded—Requirements for Recording. The data must be blocked at no more than 32,760 bytes per block.

(iii) Tape cartridges may be DLT tape IV cartridges that must be recorded in an uncompressed format and written to the tape using a Tape Archive (TAR) utility. The data must be blocked at no more than 32,760 bytes per block and must conform to the standards cited in the table as follows:

<table>
<thead>
<tr>
<th>If you are copying the record on . . .</th>
<th>. . . then, the standard below applies.</th>
</tr>
</thead>
<tbody>
<tr>
<td>DLT tape IV with a DLT 4000 drive.........</td>
<td>ISO/IEC 15307, Information technology—Data interchange on 12.7 mm 128-track magnetic tape cartridges—DLT 4 format (20 GB native, 40 GB compressed, 1.5 MB/sec).</td>
</tr>
<tr>
<td>DLT tape IV with a DLT 7000 drive.........</td>
<td>ISO/IEC 15896, Information technology—Data interchange on 12.7 mm 208-track magnetic tape cartridges—DLT 5 format (35 GB native, 70 GB compressed, 5.0 MB/sec).</td>
</tr>
<tr>
<td>DLT tape IV with a DLT 8000 drive.........</td>
<td>ISO/IEC 16382, Information technology—Data interchange on 12.7 mm 208-track magnetic tape cartridges—DLT 6 format (40 GB native, 80 GB compressed, 6.0 MB/sec).</td>
</tr>
</tbody>
</table>
each scheduled records transfer based on certain criteria (file size, FTP transfer rate, record classification, etc.). Agencies interested in sending electronic records scheduled for transfer to NARA through FTP must contact NARA’s Electronic and Special Media Records Services Division (NWME), 8601 Adelphi Rd., College Park, MD 20740-6001 or by email to cer@nara.gov to initiate the transfer discussions.

(iv) Each permanent electronic records transfer must be preceded with a signed Agreement to Transfer Records to the National Archives of the United States (Standard Form 258) sent to the Office of Records Services—Washington, DC (NWME), 8601 Adelphi Road, College Park, MD 20740-6001.

(4) Incorporation by reference. The standards cited in Sec. 1228.270(c)(1), (2), and (3) are available from the American National Standards Institute, 11 West 42nd Street, 13th floor, New York, NY 10036. The standards cited for CD-ROM, FTP, and DLT tape IV are also available from the National Information Standards Organization (NISO), Press Fulfillment, P.O. Box 451, Annapolis Junction, MD 20701. All these standards are also available for inspection at the Office of the Federal Register, 800 North Capitol Street, NW., Suite 700, Washington, DC. This incorporation by reference was approved by the Director of the Federal Register in accordance with 5 U.S.C. 552(a) and 1 CFR part 51. These materials are incorporated by reference as they exist on the date of approval and a notice of any change in these materials will be published in the Federal Register.

John W. Carlin,
Archivist of the United States.

[FR Doc. 02-16047 Filed 6-25-02; 8:45 am] 
BILLING CODE 7515-01-P
A

access time. The average time a computer searches to find information in memory or to retrieve it from a storage device.

active record. In the context of electronic records retention, an electronic document or discrete item of data that is frequently referred to and thus must be retained in primary storage devices for quick retrieval in the conduct of an organization's current business.

American Standard Code for Information Interchange (ASCII). The most popular coding method used by small computers for converting letters, numbers, punctuation, and control codes into digital form. Once defined, ASCII characters can be recognized and understood by other computers and communications devices; thus, ASCII provides a good method for the long-term retention of electronic records to ensure their future processibility on a variety of computing devices.

application. A general term used to describe a separate and discrete business process and accompanying body of data processed and managed in a computing environment.

application portfolio. A listing of all computer applications used in an organization. A model that draws a visual analogy between the functions of the organization and data processing to identify manual processes that could benefit from automation.

archival permanence. In the context of electronic records retention, the ability of records media to retain its information content in usable form permanently or for very lengthy periods of time. Archival permanence of electronic records is a function of both the stability of the records media and the longevity characteristics of the hardware, software, documentation, and other resources required to process the data residing on such media.

archiving. The process of moving copies of less-frequently accessed electronic records from primary on-line storage devices to secondary storage media for long-term storage. Archiving may take place automatically by a predetermined time period, predetermined level of file activity on the primary on-line storage device, or at the user's request.

B

backup. A duplicate copy of a computer program, a disk, or data (noun). To make a copy of a program, disk, or data (verb—back up). This process generally occurs as part of a disaster recovery program designed to provide for off-site protection and security of business-critical data. The primary purpose is to ensure the capability of recovering data when on-line processing is interrupted or when a data loss occurs.

bits per inch (bpi). A measure of the density of data on magnetic tape.

byte. A unit of data almost always consisting of 8 bits. A byte can represent a single character such as a letter, a digit, or a punctuation mark. One page of typed text requires about 2,400 bytes of storage.

C

compact disk (CD). A standard medium for the storage of digital data in machine-readable form, accessible with a laser-based reader. CDs are faster and more accurate than magnetic tape for data storage.

compact disk–read-only memory (CD-ROM). An optical disk that can be read only; it cannot be written on. CD-ROMs can store in excess of 600 megabytes of data on a single platter, and they can only be written to in one session.

compound document. An electronic document that contains information in several formats (text, graphics, or image data) and/or is assembled from several sources of an organization’s computing environment.

computer-output microfilm (COM). A type of microfilm produced by converting computer digital data to human-readable language onto microfilm; the capability to produce microfilmed images (most often on microfiche) directly from computer-generated signals.

computer-output to laser disk (COLD). The process of transferring computer data onto an optical disk; the capability to produce laser disk images directly from computer-generated signals.
**cost / risk / benefit analysis.** The concept that records should be retained for predetermined periods of time based on the cost, risks, and benefits of retaining or destroying the records and how these factors decline, expire, or increase during the life cycle of the records.

**D**

**data.** A general term used to denote computer-based records or information.

**data archives.** Copies of computer-based records on disks, CD-ROM, magnetic tapes, or other secondary storage devices for long-term storage and/or data backup as protection against the risk of loss.

**database.** A collection or body of computer data, consisting of at least one file or group of related files, usually stored in one system or subsystem and made available to one or more users for specific applications.

**data compression.** A software or hardware process that reduces computer data or images so that they occupy less storage space and can thus be transmitted faster and easier. Generally accomplished by removing the bits that define blank spaces and other redundant data and replacing them with an algorithm that represents the removed bits, thereby requiring less storage space.

**data files.** Computer-processible files that store numeric data (and sometimes data in text format) as quantitative values, which permits the numbers to be manipulated using arithmetic computations.

**data flag.** A device for identifying the point in time when electronic records make their life cycle transition from an active to semiactive or inactive status and are thus eligible for migration from primary to secondary storage media or, in some cases, immediate destruction.

**data mining.** A computing strategy similar to data warehousing.

**data set.** A separate, discrete body of computer data that is logically related, serves a common purpose or function and thus can be considered as a separate unit for analysis. Sometimes considered to be synonymous with electronic records series.

**data transfer.** The movement of data inside a computer system.

**data warehousing.** A computing strategy (effectuated by special data warehousing software) that attempts to optimize the business value of an organization’s electronic records on an enterprise-wide basis by assembling records from various applications, platforms, and storage devices into formats for presentation to management for decision-making or other business purposes.

**deletion, data.** The process of removing the index pointers to computer-based records; the actual *measure* of the electronic records themselves may or may not be accomplished during this process. Data deletion may occur with or without human intervention, and it should be accomplished under an electronic records retention policy, effectuated by records retention schedules, or as a separate act. See also purge, purge routines.

**digital.** The use of binary code (ones and zeros) to record information onto magnetic media. Any information (text, graphics, audio, video) that has been translated into binary code.

**direct-access storage device (DASD).** A computer storage device (usually a disk drive) providing direct, on-line access to electronic documents and data; computer storage devices that can respond directly to random requests for information.

**directory.** The structure in which personal computer-based electronic records are organized into logical groups, with an index or table of contents listing all documents and files contained within the directory, to facilitate access and use of the records.

**discovery.** The legal process that permits parties involved in a legal proceeding to obtain records and information relevant to the proceeding that are in the possession of another party.

**disk drive.** A device that spins a magnetic or optical disk so that data can be stored on it or retrieved from it.

**E**

**electronic archives.** Historically valuable records that exist in machine-readable or computer-processible form.

**electronic document.** A record stored on electronic storage media that can be readily accessed or changed; the smallest unit of filing within a computer application or database; a collection of discrete computer-based information objects formatted for presentation to an end-user.

**electronic imaging.** The process of capturing, storing, and retrieving documents or data, regardless of its original format, using micrographics or optical disk technologies.

**electronic mail (E-mail).** A message transmitted electronically from one computer terminal to one or more such devices via standard software and telecommunications channels. A system that enables users to compose, transmit, receive, and manage electronic messages and images across networks and through gateways connecting to other local area networks.

**electronic record.** A record containing machine-readable, as opposed to human-readable information, and consisting of character-coded electronic signals that can
be processed and read by means of computers. A record stored on electronic storage media.

electronic records inventory. An identification, description, and quantification of all computer-based records maintained by an organization, generally by application or other discrete bodies of electronic records stored in various computing environments.

electronic records retention. The act of retaining computer-based records in digital storage media because they are presumed to be needed for some current or future business purpose; such retention should occur under a formal electronic records retention program or policy.

electronic records retention program. The component of an organization's larger records management program that provides policies and procedures specifying the length of time that computer-based records must be maintained.

electronic records retention schedule. A comprehensive list of electronic records series titles, indicating for each series the length of time it is to be maintained. It may include retention in active office areas, inactive storage areas, and when and if such series may be destroyed or formally transferred to another entity such as an archives for historical preservation. A document prepared as a part of an organization's records retention program.

electronic records series. A group of related electronic records filed / used together as a unit and evaluated as a unit for retention purposes. It is logically related, serves a common purpose or function, and can thus be considered as a separate unit for purposes of developing an electronic records retention schedule. Sometimes considered synonymous with data set or with larger collections of electronic records in an application or database.

extended binary coded decimal interchange code (EBCDIC). A coding scheme that specifies bit patterns for computer-processible information for electronic records created on IBM mainframe and other large computers.

extensible markup language (XML). A flexible, nonproprietary set of standards for tagging information so that it can be transmitted using Internet protocols and readily interpreted by disparate computer systems.

G

gigabyte. A measure of electronic data storage capacity; 1,024 megabytes of computer data.

H

hard disk. A rigid metallic platter coated on both sides with a thin layer of magnetic material, permanently installed or “fixed” into a computer’s disk drive and used for the storage of digital data; a direct-access storage device. Also referred to as a fixed disk.

hierarchical storage management (HSM). A data storage management strategy in which special HSM software is used to separate active and inactive computer data by migrating files between primary and secondary storage media based on access needs, available storage capacity, costs, or other factors. The most active files and applications remain on-line in direct-access storage devices, while less frequently accessed data are migrated to near-line optical storage media, or off-line to magnetic tapes.

hyperlink. A connection between an element in a hypertext document, such as a word, phrase, symbol, or image, and a different element in the same document, in another hypertext document, in a separate file, or in a script. The user activates the link by mouse-clicking the linked element, which is usually highlighted in some way.

hypertext. Text linked together in a complex, nonsequential web of associations in which the user can browse through related topics. A hypertext document contains links to other documents and thus can be read in multiple dimensions.

hypertext markup language (HTML). The markup language used for creating documents on the World Wide Web; the formatting tool that enables text files to be linked and viewed by using Web browsers.

hypertext transfer protocol (HTTP). The client / server protocol used to access information on the World Wide Web.
**image files.** Electronic records that contain computer-processible images of documents or data stored on optical or magnetic media.

**inactive records.** Records that do not have to be readily available but must be kept for legal, fiscal, or historical purposes. Documents or data that have made their life cycle transition to closed status or otherwise are infrequently referred to and can thus be considered for continuing retention on a secondary storage device or purged from the system entirely if they have no further value.

**information.** Data that have been given value through analysis, interpretation, or compilation into a meaningful form.

**information life cycle.** The period of time from the creation or receipt of a record through its useful life to its final disposition; i.e., destruction or permanent preservation. In electronic recordkeeping environments, the transition of documents or data from active to inactive status, which is generally coincident with migration of information from primary to secondary storage media and subsequent purging or permanent preservation as electronic archives.

**Internet.** The worldwide collection of networks and gateways that allows public access to send, store, and receive electronic information. At the heart of the Internet is a backbone of high-speed data communication lines between major nodes or host computers, consisting of thousands of commercial, government, educational, and other computer systems that route data and messages. It is a network of networks.

**intranet.** A private Internet network set up within an organization behind a firewall for use, depending on security clearance, by employees, business partners, customers, or general Internet users. It usually employs Web pages for information dissemination and intranet applications such as Web browsers.

**J**

**jukebox.** A near-line storage device that houses multiple optical disks or tapes and has one or more drives that provide automatic on-line access to the information contained therein.

**K**

**kilobyte (K or KB).** A measure of electronic data storage capacity; 1,024 bytes of computer data.

**L**

**legacy system(s) / data.** A general term referring to computers and related hardware, software, and data that remain in use after the using organization has installed newer technologies and systems.

**legal retention considerations.** A term that refers to a number of legal issues that may indicate how long an organization should retain certain of its records so that it can successfully defend itself against litigation actions, enforce its legal rights, or meet its other legal obligations and needs.

**legal retention research.** The process of identifying and interpreting the laws and regulations promulgated by all jurisdictions that contain records retention requirements with which an organization must comply, and assessing other legal considerations that may be relevant to the records retention decision-making process.

**limitation of assessment.** The period of time after a tax return is filed or the tax becomes due during which a taxing agency retains the power to audit the return to verify the amount of taxes owed. This time period is often considered a relevant factor in making records retention decisions concerning the various types of financial records that may be subject to audit.

**local area network (LAN).** A data communication network of computing devices within a defined and relatively limited geographic area that permits the sharing of electronic records and other computing resources by all users having access to the network.

**M**

**magnetic media.** Various recording media coated with magnetic material on which data can be stored by selective magnetization of portions of the surface. The most common magnetic media are fixed (hard) disks, magnetic tape, and floppy disks.

**magnetic tape.** A strip of plastic film coated with a magnetic recording material and wound onto reels of various sizes onto which electronic records are recorded by means of electrical pulses; a sequential storage medium in which the next bit of data is recorded after the last bit. Subsequent retrieval is by means of serial search rather than random access.

**magneto-optical (MO) disk.** A type of optical disk that combines features of both magnetic and optical storage, thereby permitting the erasure and rewriting of documents and data in areas of the disk occupied by previously recorded information.

**mainframe computer.** A large, centralized computer typically used for enterprise-wide data processing. Also referred to as a host computer.

**markup language.** A language consisting of codes used for indicating layout and styling, such as boldface, italics, paragraphs, or insertion of graphics, in a text file; for example, HTML, XML, or SGML.

**media refreshing.** The process of periodically copying or recopying digital data onto new storage media prior to
the expiration of the expected media life spans to ensure the integrity and preservation of the data.

**media stability.** The extent to which a given recordkeeping medium retains its original physical and chemical properties; the ability of various records media to retain their information content in usable form over a given period of time.

**megabyte (MB).** A measure of electronic data storage capacity; one million bytes of computer data; usually 1,048,576 bytes; 1,024 kilobytes; 1,024 megabytes equal one gigabyte.

**metadata.** Data about or describing other data; data about data elements or attributes (name, size, data type, etc.); about records or data structures (fields, columns, etc.); about data (where is it located, how it is associated, ownership, etc.)

**migration, data.** (1) In traditional data processing, the process of moving or copying data between a variety of computer storage devices based on media capacity, access time, and frequency of user requests for the data. (2) In digital archives management, a set of tasks designed to achieve the periodic transfer of digital materials from one hardware / software configuration to another, or from one generation of computer technology to another for the purpose of assuring the preservation and integrity of the data in rapidly changing technology environments without having to undergo a major conversion or re-inputting of data.

**N**

**near-line storage.** Computer data available on a secondary storage device for rapid user access but at a slower rate than would be provided by direct-access, on-line storage devices.

**network.** A group of computers and associated devices connected by communications facilities, thereby enabling the computers to share data and files.

**nonremovable media.** Magnetic or optical disk storage devices that are “fixed” within disk drives and are not intended to be removed for off-line storage. These media provide very rapid, on-line processing and retrieval of electronic records.

**O**

**off-line storage.** Electronic records stored on media located apart from the computer device on which it will be retrieved and processed; data that is not physically stored on an accessible drive such as removable tapes or disks.

**on-line storage.** Electronic records stored on media housed on magnetic or optical disk drives within a computer system, thus permitting very rapid access and continuous processing; data that is available on a primary storage device.

**operating system.** The software that controls the allocation and usage of computer hardware resources such as memory, CPU time, disk space, and peripheral devices.

**optical disk.** A high-density information storage medium where digitally encoded information is both written and read by means of a laser. Platters are available in erasable and nonerasable formats.

**personal computer (PC).** A microcomputer that conforms to the standard developed by IBM Corp., which uses an Intel or compatible microprocessor. The major device used to create electronic records at the individual desktop level in offices.

**portable document format (PDF).** A proprietary software product that has become a de facto standard for providing universal access to electronic documents over the Internet. Created by Adobe Systems, the portable document file format preserves all fonts, formatting, graphics, and color of any source document, regardless of the application used to create it.

**permanent record.** A record, regardless of form or media, that is required by law to be retained indefinitely or which has been designated for continuous preservation because of reference, historical, or administrative significance to an organization. Electronic records that require permanent preservation must be in computer-processible format.

**petabyte.** A measure of electronic data storage; one thousand terabytes of computer data. This extremely large measure of computer data is often used to express the quantity of electronic records on a nationwide or global basis.

**platform.** A general term used to refer to the type of operating systems and other major features of the hardware and software used in a given computing environment.

**portal.** A Web site that serves as a gateway to the Internet. A portal usually offers a search engine and links to useful pages.

**purge.** To remove information from a file that has no further value, usually according to an electronic records retention schedule, effectuated by the use of purge routines incorporated into the design criteria of a computer application. Active and inactive records may be purged.

**purge routine.** Any set of programmed instructions, built into applications programs or installed as a system-wide utility, to identify inactive records and remove them from data files. These actions should occur under the authority of an electronic records retention schedule.
R

record. Recorded information, regardless of medium or characteristics, made or received by an organization that is evidence of its operations and that has value requiring its retention for a specific period of time; a collection of related data fields in a computer database; the basic organizational unit of the database, consisting of a group of facts about a particular subject.

recordkeeping system. A manual or automated system in which records are collected, organized, and categorized to facilitate their preservation, retrieval, use, and disposition.

records media. A general term referring to the material on which business information has been recorded and may subsequently be used for business purposes.

records appraisal. The process of evaluating records based on their current administrative, regulatory, historical, legal, and fiscal use; their archival and informational value; their arrangement; and their relationship to other records, generally accomplished as part of the process of developing records retention schedules. In electronic records retention, records appraisal is the evaluation of the worth or value of a collection of computer-based records for retention purposes, based upon the current or predicted future use(s) of the information, among other criteria.

records disposition. The final action for records when they reach the end of their retention in active and/or inactive storage (i.e., the records are either destroyed if they have no further value, or they are preserved permanently as archival materials). These actions should occur under authority of a records retention program.

records management. The systematic control of all organizational records during the various stages of their life cycle: from their creation or receipt, through their processing, distribution, storage and retrieval, maintenance and use, to their ultimate disposition.

records retention. The act of retaining business records for predetermined periods of time commensurate with their value, with subsequent disposal or permanent preservation as a matter of official policy.

records retention program. A program established and maintained to provide retention periods for records in an organization. The component of a records and information management program that provides policies and procedures specifying the length of time an organization's records must be maintained. The program provides for the systematic destruction of records that no longer serve any useful purpose and is implemented by effecting the destruction of records on a scheduled basis, as specified in the organization's records retention schedules. The program also provides for the permanent preservation of records considered to possess historical or archival value, again as specified by the records retention schedules. The records retention program is one of the organization's major tools for controlling the growth of its records, and it also minimizes the legal risks that can be associated with maintaining and destroying business records.

records retention schedule. A comprehensive list of records series, indicating for each series the length of time it is to be maintained, and when such series may be reviewed for destruction or archival retention. It often indicates retention in active and inactive storage areas.

records series. A group of related records that are normally filed together as a separate unit and which therefore permits evaluation as a unit for retention scheduling purposes. See also electronic records series.

refreshing, data. A procedure used to maximize the life expectancy of computer storage media and the data residing on them.

removable media. Magnetic or optical storage devices that may be removed from and stored apart from the disk drives on which they are recorded and read.

retrieval. The process of obtaining desired information from a recordkeeping system. The action of accessing information from stored data on a computer system.

S

server. A computer running software that controls access to a computer network and its resources such as printers and disk drives.

statutes of limitation. Laws containing provisions specifying the time during which a party can sue or be sued on a matter. Business records are often considered to possess varying degrees of legal value during this time period, and decisions to retain or destroy them are often based on this value.

storage capacity. The amount of data that can be contained in an information holding device; in computer storage media, storage capacity is generally expressed in terms of bytes (megabytes, gigabytes, terabytes, petabytes, etc.).

subdirectory. A directory that is inside or subordinate to another directory. Users reach a subdirectory by going through all directories above it. Used in organizing and managing personal computer-based electronic records in cases in which file contents become too large or cumbersome for effective processing and retrieval.

T

tape rotation back-up system. A method of protecting vital computer-based records by periodically storing copies of magnetic tapes containing updated vital data in a secure facility remote from an organization's computer processing facility.

terabyte. A measure of electronic storage media capacity; one thousand gigabytes; the largest computer storage systems can accommodate this quantity of data.
text files. A collection of computer-based electronic records typically consisting of character-coded alphabetic and graphic symbols commonly encountered in typewritten documents. Text files may be created by word processing programs or other computer software.

U

uniform resource locator (URL). An Internet address that directs a Web browser to locate a resource.

V

virtual memory. A technique for handling programs too large to fit entirely into a computer’s memory; programs and data are divided into segments that are stored on disk or tape and loaded into memory only as needed for a program’s execution.

visible records media. Records media whose information contents are human-readable and do not require processing by computer hardware and software; specifically, paper and microfilm records.

voice mail. A computerized answering service that records a digitized telecommunications message that can be stored and subsequently retrieved in audio or visual format.

W

Web browser. A client application that enables a user to view HTML documents, follow the hyperlinks among them, transfer files, and execute programs.

World Wide Web. A system of interlinked hypertext documents residing on Web, or HTTP, servers throughout the world.

write once, read many (WORM). An optical disk on which data is recorded or written once and can be read repeatedly but never changed or erased.
As is discussed in this book, computer technology and all that comprises it, including its content, is often shifting and disappearing. Nevertheless, where we have used the Web as a source, we have generally provided URLs indicating that source. We caution our readers, however, that the life expectancy of these sources may be shorter than that of this book.

**Electronic Records Management / Retention – General**


Data Storage Management


**Legal Issues in Electronic Records Retention**


“Storage Will Be 75% of All IT Spending Over the Next Couple of Years.” Storage Inc., Quarter 1 2001.


E-mail Retention and Management


“E-Mail @ 30.” Computerworld, 12 November 2001.


Kontzer, Tony. “More Than an In-box: E-mail is Moving to a Broader Business Purpose.” Informationweek, 6 May 2002.


Schneider, Dan. “E-mail: Just Another Record.” e-doc, March/April 2001.

Shinkle, Tim. “Changing Technology Requires a New Look at Enterprise E-mail Management.” Storage Management Solutions 6, no. 3 (2001).


Tebbe, Mark. “Watch Out: E-mail Trails Can Easily Turn Your Own Written Words Against You.” InfoWorld, 1998.


Records Management / Document Management Software


**Long-Term Data Retention / Digital Preservation**


---

**Presentations at ARMA Conferences**


University of Pittsburgh Project. “Functional Requirements for Evidence in Recordkeeping.” Available at www2.lis.pitt.edu/~sochats/nhrpc.html.


The Web and Electronic Records Retention


INDEX

A

access restrictions, 70
access time, 30
acclimatization, 79
administrative values, 24
aftermath, lessons learned, 21
air-conditioned storage facility, 78
application, 10
application portfolio, 32
archival data, appraisal of, 70
archival permanence, 72
archiving, 12, 30
ASCII, 70
ASCII format, 75
Australian Tax Office, 156
authenticity, 76

B

bits per inch (bpi), 74
blank media stock, storage of, 77
business case, logic of, 9
business case, other side of, 12
business-critical application, 46

C

CD-ROM media, 74
Code of Federal Regulations, National Archives and Records Administration, 94
comments about specific questions, 34
compact disk (CD), 74
complete deletion, 81
comprehensive data retention functionality, 81
computer applications managed by IT departments, 29
computer data storage, 30
computer-output microfilm (COM), 27
computer-output to laser disk (COLD), 27
conclusion, 57
conduct interviews, 36
content over format concept, primacy of, 24
content, 76
cost/risk/benefit concept, 24

data, 27
data archiving and backup, 30
data collection survey instrument, 32
data compression, 76
data elements, survey form, 32
data file, 75
data flag, 34, 81
data for preservation, select, 72
data life cycle management, missing element in, 2
data migration, 4, 9
data migrations, perform, 74
data mining, 13
data of permanent value, preservation of, 2
data of temporary value, disposal of, 2
data owners, 4
data purge functionality, 4
data purge routines, 81
data purging, 34, 81
data retention audits, 83
data retention functionality, 82
data retention or purge days, 83
data retention, when not a problem, 3
data set, 23
data storage and retention problem, 9
data storage costs, reducing, 11
data transfer, 66
data transfer/accessioning, 70
data warehousing/mining software, 13
data, solicit from, 32
database, 36
desktop records retention, general principles for, 40
desktop retention methodology, executing, 41
desktop retention, 40
desktop, the, 40
desktop users’ guide, 42
digital format, 1
digital media, 26
digital media stability, 67
digital preservation, 64
digital preservation, accepting responsibility for, 66
digital preservation problem, pervasiveness of, 65
directory, 40
discovery, 15
disk drives, 30
document destruction, 56
document profiles, 55
DoD 5015.2-STD, 101
DoD Foreword, 100
DoD standard, 54

E
electronic and special media records services division, case study, 69
electronic document, 46
electronic document imaging systems, 57
electronic document management software, 55
electronic imaging, 53
electronic mail (e-mail), 46
electronic records, controlling growth of, 11
electronic records retention, 1, 2, 9
electronic records retention and risk management, 16
electronic records retention and future of records management, 13
electronic records retention and IT environment, 30
electronic records retention at desktop level, 12
electronic records retention, benefits of, 10
electronic records retention, define, 23
electronic records retention, new IT policy for, 83
electronic records retention program, 12
electronic records retention schedule, 10, 23
electronic records retention scheduling, principles for, 23
electronic records retention, selling the business case, 9
electronic records retention, when does not exist, 2
electronic records series, 23
electronic retention periods, integrate, 38
Electronic Signatures in Global and National Commerce Act, 117
e-mail management at ABC Corporation, case study, 51
e-mail mismanagement, 47
e-mail problem, magnitude of, 46
e-mail problem, records management aspects of, 48
emulation solution, 68
emulation, 68
emulator, 68
Enron and Arthur Andersen, case study, 19
ensuring compliance with laws and regulations, 16
enterprise retention schedules, 38
e-paper, 69
E-Sign Law, 17
E-Sign, records retention provisions of, 17
exercising, 79
extended binary coded decimal interchange code (EBCDIC), 70
extensible markup language (XML), 61, 75

F
field, 76
file, 49
file formats, standardize, 75
file transfer protocol (FTP), 70
floppy disks, 44
future, the, 70

G
gigabyte, 30
greatest threat: people, not technology, 67

H
hard disk, 31
hardware and software vendors, 4
HD-Rosetta, 68
hierarchical storage management (HSM), 13, 25, 31
high-density, read-only memory (HD-ROM), 68
historical value, 24
history of neglect, why, 3
hyperlinks, 60
hypertext markup language (HTML), 60
hypertext, 60

I
image file, 75
inactive record, 34
information technology departments, 3
Internal Revenue Service, 88
Internet, 55
InterPARES Project, 69
intranet, 55, 60
introduction, 1
IRS Revenue Procedure 98–25, 18
ISO 15489 and records retention, 4
ISO 15489: data preservation practices, 72
ISO 15489 methodology, 25
IT department, obtain cooperation/participation of, 31
IT specialists, working with, 29
jukebox, 31

kilobyte, 46

legal exposure, reducing, 15
legal issues, 15
legal issues and risks, 48
legal retention considerations, 39
legal retention requirements, determine, 37
legislation, new, 17
long-term data retention, 27
long-term data retention, introduction, 64
long-term data retention, sample policy, 73
long-term data retention, technical guidelines and best practices, 72

magnetic diskettes, 67
magnetic media, 74
magnetic tape, 10, 31, 67, 74
magneto-optical (MO) disks, 74
mainframe, 29
management and retention of e-mail, sample policy, 48
management issues, 50
markup languages, 75
media acclimatization, 79
media inspection, 79
media recopying, 78
media refreshing/rewinding, 79
media shelving/housing, 78
media stability, 67
media storage, ANSI standard for, 77
media types, stability of 67
medium-length data retention, 27
megabyte, 11
metadata issues, address, 27, 76
metalanguage, 75
microfiche, 67
microfilm, 67
most severe manifestation, 66

NARA, Expanding Transfer Options for Electronic Records, 174
NARA, General Records Schedule 24, 167
NARA file format guidelines, 75
NARA media guidelines, 74

NARA requirements, 77
National Archives and Records Administration, 163
near-line retention period, 25
network attached storage (NAS), 30
no ideal solution, 65
nonerasable media, 57
nonremovable media, 44

official vs. nonofficial records, 41
off-line retention period, 25
on-line and near-line archiving, 30
on-line retention period, 25
operating systems, 13
operational value, 24
optical media, 57, 67
other data retention capabilities, 81

paper, 67
permanent data, maintenance of, 70
permanent e-mail, 69
permanent retention periods, assigning, 26
permanent storage media, new, 68
personal computer (PC), 40
petabyte, 11
platform, 13, 34
portable document format (PDF), 61, 75
portal, 61
primary value, 24
production application data for retention, scheduling, 31
proper media maintenance tasks, perform, 78
purge, 4
purge functionality, 35, 81
purge retention functionality, when to incorporate, 82
purge routines, 32

reappraisal to nondigital/nonpermanent status, 74
recordkeeping at the crossroads of change, 1
records appraisal concept, 24
records disposition, 40
records management, 2, 53
records management software, 53
records managers, 4
records retention, 1
records retention at the desktop level, sample policy, 42
records retention functionality in EDMS solutions, 56
records retention, general corporate, sample policy, 5
records retention, general policy for, 5
records retention program, 15
records retention requirements specified in DoD 5015.2-STD, 58
records retention schedule, 1, 2
records retention vs. information life cycle management, 13
records series concept, apply, 23
refreshing, 79
reliability, 76
removable media, 30
research value, 24
retensioning, 79
retention functionality, incorporate, 28
retention issues, 50
retention media, utilize COM or COLD, 27
retention of Web pages, sample policy, 61
retention options concept, 24
retention periods and schedules as organizational policy, 38
retention periods, assigning, 56
retention periods, determine 24
retention periods, need for consistency, 26
retention policy, implementation of, 2
retention policy issues, 56
retrieval, 43
Revenue Canada, 151
Revenue Procedure 98–25, 16, 18, 88
rewritable media, 57
safety and security, 78
Sarbanes-Oxley Act, 19
secondary value, 24
server, 29
server-hosted storage, 30
skill sets required, 29
software applications records retention requirements, sample policy, 83
software retention functionality scenarios, 82
software solutions, 53
solution convergence, 55
solutions, 50
some new initiatives and potential solutions, 68
some policy recommendations, 21
statutes of limitation, 182
storage area network (SAN), 30
storage capacity, 30
storage facility, cleanliness of, 78
storage media, select appropriate, 74
store media properly, 77
stored data, overall management of, 10
structure, 76
subdirectory, 40
summarize results, 36
summary data from IT, collect, 31
survey form, test, 35
survey response and follow-up, 36
survey return information, 35
systems documentation, preserve, 76
T
tape management/disaster back-up systems, 12
tape rotation back-up system, 182
temperature and humidity conditions, 77
temporary data, implementation issues for, 81
terabyte, 10
text file, 75
total life cycle retention periods, 25
total retention period, 25
total retention periods, determine, 26
U
Uniform Electronic Transaction Act, 18, 124
United States Code, Government Paperwork Elimination Act, 147
universal resource locator (URL), 60
unprecedented challenge, 65
V
virtual memory, 183
visible media, 1
visible records media, 32
voice mail, 46
W
Web browser, 56, 60
Web content, preservation of, 61
Web sites, applying retention to, 60
Web, the, 60
WORM, 60
write once, read many, 57
X
XML, 75
David O. Stephens, CRM, FAI, CMC, is Director of the Records Management Consulting Division at Zasio Enterprises, Inc., a leading records management software and consulting firm based in Boise, Idaho. In this capacity, he directs records and information consulting studies and projects for clients in government and industry throughout the United States and in other countries.

Mr. Stephens is an internationally recognized author, speaker, and consultant. He is co-author of the Fourth Edition of Information and Records Management, Glencoe/McGraw-Hill, 1995. As a consultant since 1979, he has developed comprehensive records management programs for over 300 organizations in all types of businesses and at all levels of government.

Mr. Stephens served as President and CEO of ARMA International in 1989–1990, and he was inducted into the Company of Fellows of that organization in 1992. Mr. Stephens is a Certified Records Manager and a Certified Management Consultant. He earned a masters degree in public administration from North Carolina State University.

Roderick C. Wallace, CRM, is founder and President of Insurance Record Services, Inc., and Retention Research Associates. Insurance Records Services publishes Insurance Record Keeping Requirements, a compilation of U.S. insurance records laws and regulations. Retention Research Associates publishes Global Record Keeping Requirements, which covers records retention laws and regulations from countries around the world. Both firms also consult with industry on research and development of records retention schedules. Prior to founding his own firms, Mr. Wallace was employed as a senior systems analyst at a life insurance company and previously as corporate records manager for a manufacturer.
ARMA International is the leading professional organization for persons in the expanding field of records and information management.

As of November 2002, ARMA has about 10,000 members in the United States, Canada, and 37 other countries around the world. Within the United States, Canada, New Zealand, Japan, Jamaica, and Singapore, ARMA has nearly 150 local chapters that provide networking and leadership opportunities through monthly meetings and special seminars.

ARMA’s mission is to provide education, research, and networking opportunities to information professionals, to enable them to use their skills and experience to leverage the value of records, information, and knowledge as corporate assets and as contributors to organizational success.

The ARMA International headquarters office is located in Lenexa, Kansas, in the Kansas City metropolitan area. Office hours are 8:30 A.M. to 5:00 P.M., Central Time, Monday through Friday.

ARMA International
11880 College Blvd., Suite 450
Overland Park, Kansas 66210
800.422.2762 ● 913.341.3808
Fax: 913.341.3742
www.arma.org