1997

Audit implications of electronic document management; Auditing procedure study;

American Institute of Certified Public Accountants

Canadian Institute of Chartered Accountants

Auditing
Procedure
Study

AICPA

AMERICAN INSTITUTE OF CERTIFIED PUBLIC ACCOUNTANTS

Audit Implications of Electronic Document Management

Published by the
American Institute of Certified Public Accountants
in cooperation with the
Canadian Institute of Chartered Accountants

Audit Implications of Electronic Document Management
AICPA

Auditing
Procedure
Study

AICPA

AMERICAN INSTITUTE OF CERTIFIED PUBLIC ACCOUNTANTS

Audit Implications of Electronic Document Management

Published by the
American Institute of Certified Public Accountants
in cooperation with the
Canadian Institute of Chartered Accountants

Statement of Policy

Auditing Procedure Studies are issued by AICPA Audit and Attest Standards and are part of the research program of the American Institute of Certified Public Accountants (AICPA). Each study is designed to inform auditors of developments and advances in auditing procedures. The studies present the views of the author or study group.

Auditing Procedure Studies are intended to provide practitioners with nonauthoritative practical assistance concerning auditing procedures. Comments on this study should be addressed to the Institute's director of audit and attest standards. Comments will be treated as public information unless a writer requests that his or her comments be kept confidential.

This Auditing Procedure Study has not been approved, disapproved, or otherwise acted on by the Auditing Standards Board, the membership, or the governing body of the AICPA. Therefore, the contents of this study, including the recommendations, are not official pronouncements of the Institute.

ISBN 0–87051–189–0

1 2 3 4 5 6 7 8 9 0 AAS 9 9 8 7

Audit Implications of Electronic Document Management

FOREWORD

The primary objective of this study is to discuss the opportunities and challenges presented to the auditor by electronic document management (EDM). It covers a number of issues that the auditor will encounter when involved with EDM. The study was prepared by a Study Group comprising members of the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA).

The Study Group's terms of reference were to discuss the:

- technology and its important uses;
- impact on the audit approach — tests of controls vs. substantive approach;
- business risks and audit risks associated with using the technology;
- pre-implementation considerations;
- controls that are important in EDM systems;
- effect of the potential loss of the traditional paper audit trail;
- forms of audit evidence that are available;
- use of computer-assisted audit techniques;
- legal considerations.

Appreciation is expressed to the chairman and members of the Study Group for their efforts in producing this study. Thanks are also expressed to Jane M. Mancino, CPA, of the AICPA for her participation in the project and to Donald E. Sheehy, CA, Senior Manager, CICA Research Studies, who, at the direction of the Study Group, undertook the research and drafting of the study.

Thomas Ray, CPA,
Director, Audit and Attest Standards
American Institute of Certified
Public Accountants

David J. Moore, CA,
Research Studies Director,
Canadian Institute of
Chartered Accountants

April, 1997

STUDY GROUP

Chair
Ray Grenkie, CA
Coopers & Lybrand Consulting
Toronto, Ont

Members
John R. Adshead, CA
Office of the Auditor General
Ottawa, Ont.

Carol A. Langelier, CPA
United States General
Accounting Office
Washington, D.C.

Yezdi N. Pavri, CA
Deloitte & Touche
Toronto, Ont

J. Donald Warren, Jr., CPA
Coopers & Lybrand L.L.P.
New York, N.Y.

Staff
Donald E. Sheehy, CA
CICA
Toronto, Ont

Jane M. Mancino, CPA
AICPA
New York, N.Y.

TABLE OF CONTENTS

Chapter 1

INTRODUCTION TO STUDY

This introductory chapter provides background discussion on electronic document management and discusses its general audit impact.

INTRODUCTION TO ELECTRONIC DOCUMENT MANAGEMENT (EDM)

Growth of the Paperless Office

In the 1960s, the vision of the paperless office promised that document information could soon be shared electronically. Information would be transmitted instantaneously, always available when and where it was needed, vastly improving office productivity. In the 1970s, many believed the paperless office was just around the corner. They got it exactly backward: in the 1980s, computers, laser printers and high-speed copiers flooded companies with documents. This continued into the 1990s. In the early 1990s, 95% of business information was still on paper, and office workers spent 15-30% of their time searching for information that has been moved, filed or stored. 1

Unfortunately, information stored on paper is hard to sort, search, share, transmit, and retrieve, but easy to misfile, expensive to copy and typically located somewhere other than where it is actually needed. These limitations have determined the design of business processes from transaction processing, accounting and engineering, to customer service, claims management and archival storage. 2

Recent advances in technology and electronic communications have had a significant impact in this area. Two trends have evolved that are changing traditional business practices: 3

- more electronic documents are being created, through the use of word processing and other types of end-user software, by mobile and home-based work forces, and transmitted through increased use of e-mail; and
- increased use of electronic capture of the remaining paper-based documents by digital scanning, or imaging.

The concept of the paperless office has been revived with the rapid evolution of document imaging technology. EDM has made file cabinets obsolete in

paper-intensive operations such as banks, hospitals, insurance companies, governments and other large entities. Increasingly, the technology is moving beyond those markets, finding application in businesses of all types and sizes. For some users, an EDM system has been part of a broader reengineering process. For others, EDM has been added to modify and enhance existing applications.

4 One reason for this growth in EDM is that costs are plummeting, partly due to the fact that general-purpose PCs have become powerful enough to serve as workstations in all but the most demanding situations. Also, PC operating systems and application programs are becoming powerful with easier to use interfaces. These are discussed in more depth in Chapter 3.

Example 1 — EDM in a loan application situation

EDM applications can be used to control the processing of a loan application in a lending institution by electronically routing the transaction directly to appropriate staff for review, approval and authorization. Once authorized (electronically), the image, containing the loan application data and the authorizing signature, acts as the record for the business transaction, eliminating the need for data to be retyped and filed manually, or copied. The image can be linked to other documentation for that customer. More comprehensive records can then be built for each customer and will allow customer inquiries to be dealt with more quickly. This provides a competitive advantage and improves the quality of decision making by the entity because it identifies and uses the most economical route for the most appropriate information to reach a decision maker. Intervening levels of staff that do not add value can be bypassed.

What is a Document?

5 Historically, documents have taken the form of paper. For example, the Concise Oxford Dictionary defines a document as "thing, esp. title-deed, writing, or inscription, that furnishes evidence (esp. in law and commerce)...." Webster's College Dictionary defines a document as "a written or printed paper furnishing information or evidence...any written item, [such] as a book..., esp. of a factual or informative nature...."

6 This definition, especially given the underlying paper emphasis, is being challenged as entities move to EDM. One recent definition states that a "document is a collection of information, authored for the purpose of transferring and preserving knowledge."[1] Paper is being viewed as one means to represent a document. Electronic representation is another alternative.

[1] T.M. Koulopoulos and C. Frappaolo, *Electronic Document Management Systems a Portable Consultant* (New York, N.Y.:, McGraw-Hill, Inc., 1995), p. 28.

One view of an electronic document is set out in Exhibit 1. Documents can be a composite of images, text and other information types. Text and other information types can usually be coded. Images are generally uncoded information because they cannot be presented in granular (segmented) form. They exist in a complete state. Images can be easily retrieved only if descriptive information is added to a structured database index which is then linked to the respective image. 7

Retrieval facilities for document collections can take one of three forms: 8

- database retrieval approach — the database will act as an external index to the document, used for imaging;
- context-based retrieval — using the words, ideas and concepts expressed in the document. For example, full-text retrieval systems will index all words in the document for possible retrieval at a later date;
- structured retrieval — hybrid of the prior two, it will tag sections of the document to identify structured components of the document.[2]

What is Electronic Document Management?

Document management is the systematic movement, processing and storage of business documents ranging from correspondence to technical drawings. Historically, business information has been recorded in paper documents, stored in filing cabinets and retrieved and processed manually. Dissemination and storage procedures were based on physical handling of paper by people "pushing" or moving paper from one temporary location to another, often adding/providing information at each stage, until a permanent storage stage is reached. Electronic document management (EDM) systems provide the means to generate, disseminate and store documents electronically. They also can help to manage the flow of work, in the form of documents, through an enterprise. An example of an EDM system is set out in Exhibit 1 of Chapter 2. 9

FOCUS OF THIS STUDY

EDM systems expand the traditional processing of paper documents: 10

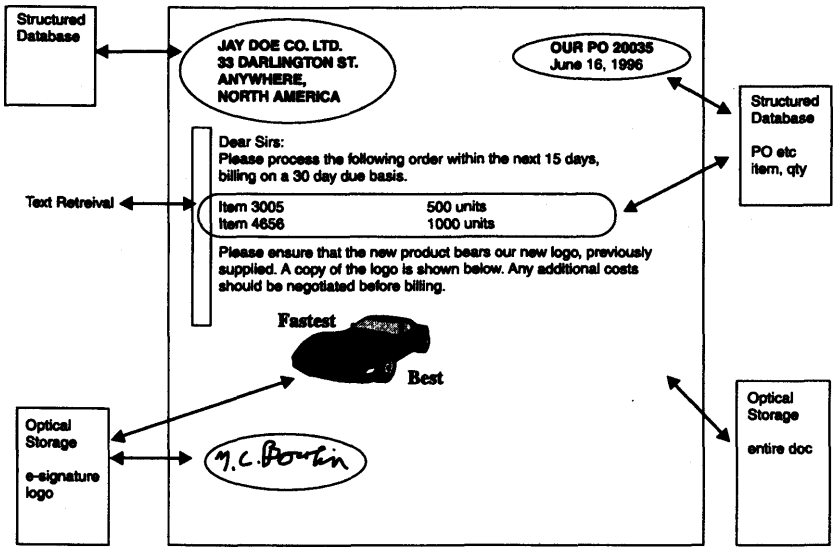
- Document management systems provide a layer of management and control over electronic documents, often existing in many different forms (for example, word processing, spreadsheets, etc.).
- Image systems can provide a bridge between paper and electronic document management. Digital images are stored in place of paper documents, microfilm, or microfiche. Imaging systems enable an entity to store and retrieve documents including charts, graphs, signature records, engineering drawings and other data.

---

[2] T.M. Koulopoulos and C. Frappaolo, *Electronic Document Management Systems a Portable Consultant* (New York, N.Y.:, McGraw-Hill, Inc., 1995), p. 30.

Exhibit 1

Representation of Electronic Document



- Text management systems can provide storage and navigation facilities for text formatted as data. Text management systems provide access to large volumes of text records that can be searched based on words, phrases or concepts.
- Workflow systems can model, implement and monitor the flow of documents through an entity to accomplish essential tasks such as filling out and processing forms, and reviewing and approving designs.
- On-line information can be shared electronically between entities through electronic data interchange (EDI).

This study addresses the first four aspects. EDI is discussed in the joint AICPA/CICA audit technique study, *Audit Implications Of EDI*, published in 1996.

GENERAL AUDIT IMPACT

11 An auditor, engaged in a financial statement audit where the financial statements and underlying information and evidence are significantly affected by the use of EDM, should understand that this audit differs from a traditional audit in two basic ways:

- the auditor is often *not* looking at the financial transaction system itself but, rather, at the support for the transaction; and
- this support may be an original document or its digitally scanned duplicate.

Relationship with Transaction Processing System

Some entities will undertake a comprehensive integrated document management solution in which the EDM system is linked to the transaction processing system(s). Others will take a more piecemeal approach, responding to specific pressures, such as the need to manage records of contacts with customers. EDM can deliver these benefits when implemented as a stand-alone system or when integrated into larger applications. Stand-alone systems are commonly found where document storage and retrieval is the primary objective and large numbers of documents are handled. Libraries and law offices are good examples of appropriate stand-alone applications of EDM. 12

In either case, the net impact is that it is easier to recall prior business transactions and correspondence. As will be discussed in the next chapter, EDM can increase staff productivity through more efficient management of workloads and a reduction in time required to store and retrieve information. Associated paper handling, archiving, copying and transfer costs can also be reduced. 13

A well-integrated system should result in significant benefits to the entity. When fully integrated with other computer systems, EDM applications can be used to control the processing of a document, direct its routing, facilitate approval and link it to any other appropriate documentation or correspondence relating to the transaction. All of the information is instantly available. A well-controlled system will also assist in maintaining document authenticity and confidentiality. 14

Relationship with Financial Transaction System[3]

One of the first and most significant issues the auditor needs to understand, when auditing a client with a new EDM system, is the type of EDM system and its interrelationship with the financial transaction system. The auditor could encounter three possible types of EDM systems: 15

- A system that is completely integrated with the financial transaction system (a *direct-impact* system), for example, where optical character recognition is used for high-speed check processing or where optical character recognition is used for invoice input directly into the financial transaction system. This is a less common scenario.
- A system that acts as support for a financial transaction system, but is not integrated (an *indirect-impact* system), for example, where EDM is used for insurance claims processing, there is typically no direct input into the financial transaction system: however, all of the support for the transaction is in the EDM system. This is a more common scenario.

---

[3] For the purposes of this study, a financial transaction system is regarded as any system that has a significant impact on the financial statements of an entity.

- A system that has no interaction with the financial transaction system (a *no impact* system), for example, a résumé system or a project information system. This is also a common scenario.

16 It is also possible to have a combination of the first two above. For example, in a mutual fund purchase application, the document is scanned into the system, an operator subsequently brings up the image on the screen, simultaneously with the financial transaction system. If the operator is satisfied that the transaction should proceed, the system is instructed to perform an electronic on-screen posting from the EDM system to the financial transaction system.

17 This study focuses on the benefits and exposures of both direct-impact and indirect-impact EDM systems. The discussions can also be applied, where appropriate, to a no-impact system.

18 Control activities in an EDM system may be introduced on a selective basis. Ideally, all the control activities that were previously included in a manual system should be incorporated into an EDM system, because there will be no physical documents after the initial creation or scanning.

Importance of Document Authenticity

19 In the opinion of the Study Group, it is very important that the entity have appropriate control activities to maintain "document authenticity." The concept of document authenticity is central to an auditor's understanding of an EDM system. Generally, documents cannot be assumed to be what they purport to be unless:

- in the case of electronically produced documents, no alterations have been made;
- in the case of scanned images of original paper documents, the scanning capture process is controlled and no subsequent alterations have been made.

It should be noted that scanning may not capture all of the information, for example, an embossing seal, from an original document.

20 If an entity has an EDM system (and particularly when it is a direct-impact system), it will likely be more effective and efficient for an auditor to establish, through tests of controls and/or substantive tests, the validity, completeness and accuracy of the information included in the EDM system (document authenticity). This will permit the auditor to subsequently use the information as evidential matter in testing the related assertions embodied in the financial statements. Alternatively, the auditor could use original documents, if available, or perform other substantive procedures. This means that the auditor may need to understand and perhaps test the controls built into the EDM system instead of the manual controls and procedures. This is discussed in detail in Chapters 4 and 6.

Audit Benefits

An EDM system offers significant benefits to the auditor conducting an audit: 21

- In traditional paper-based environments, evidence and the timing of the audit are constrained by the need to first assemble original documents and all related data (except in situations where microfilm has been used). With EDM, however, data and documents can be inspected during the regular flow of work, while documents are actually being processed. The data should also be "cleaner" due to the controls over input into the system.
- The auditor can use the system to select and prioritize samples and put them into the auditor's work queue, with all the necessary documents electronically "attached."
- The system can provide a comprehensive audit trail, covering all documents, not only financial data records, indicating which personnel performed which functions with the documents.
- The potential integration of existing and EDM systems (integrating data and paper information) should enable the auditor, with the cooperation of the client, to automate much more of the audit and to "design the audit into the system."
- It is also possible for an auditor to conduct the audit remotely, without disrupting the work of the users/employees.

Many of these points are discussed in more detail later in this study.

A client's use of EDM may affect the auditor in varying degrees. Auditors who are experienced in the use of computer-based auditing techniques and testing computer controls will likely not be challenged by EDM. Auditors who do not have expertise in this area may find that complex EDM systems do represent a significant challenge and, thus, they should consider using a specialist. 22

STANDARDS AND AUDIT ISSUES

Generally accepted auditing standards require that a sufficient understanding of internal control be obtained to plan the audit and that, when control risk is assessed below maximum, sufficient audit evidence be obtained through tests of control to support that assessment. Those standards also require that sufficient appropriate audit evidence be obtained to afford a reasonable basis to support the content of the report. 23

AICPA	*CICA*
AICPA SAS 55, amended by SAS 78, *Internal Control in a Financial Statement Audit*, states that "a sufficient understanding of internal control is to be obtained to plan the audit and to determine the nature, timing and extent of tests to be performed."	*CICA Handbook* Section 5100 states that "a sufficient understanding of internal control should be obtained to plan the audit. When control risk is assessed below maximum, sufficient appropriate audit evidence should be obtained through tests of controls to support the assessment."
AICPA SAS 55, amended by SAS 78, separately states that "Assessing control risk at below the maximum level involves • Identifying specific controls relevant to specific assertions that are likely to prevent or detect material misstatements in those assertions. • Performing tests of controls to evaluate the effectiveness of such controls."	
The third standard of field work states that "sufficient competent evidential matter is to be obtained through inspection, observation, inquiries, and confirmations to afford a reasonable basis for an opinion regarding the financial statements under audit."	*CICA Handbook* Section 5100 states that "sufficient appropriate audit evidence should be obtained by such means as inspection, observation, enquiry, confirmation, computation and analysis, to afford a reasonable basis to support the content of the report."

Audit Evidence

24 Generally, documentary evidence is more reliable than oral evidence; and external evidence is more reliable than internal evidence. Therefore, the auditor traditionally obtains some degree of assurance as to the existence and occurrence of transactions from the existence of externally generated evidence and from the indications of work done on this evidence (for example, routing stamps initialled and dated). With an EDM system, electronic evidence obtained from the client's computer system may not provide the same level of comfort in respect of existence, occurrence and completeness as externally generated paper. A well-controlled system may, however, provide for an increased level of comfort. To increase the efficiency of auditor procedures, document authenticity (see paragraph 19) is essential. As discussed in Chapters 5 and 6, this issue will affect the nature and method of audit testing conducted.

Audit Issues Addressed in this Study

25 It is the opinion of the Study Group that the following issues are the most significant for dealing with an audit of systems affected by EDM:

- Knowledge of the business is crucial; this is addressed in Chapter 4.
- Documents evidencing transactions may exist only in electronic form, but this should be compensated for by adequate IT controls; the impact on the audit is discussed throughout this document; some legal issues are discussed in Appendix B.

- The auditor may want to test controls over the conversion of items entered into the EDM system. Backfile conversion and other considerations are discussed in Chapter 3.
- The auditors assessment of control risk regarding various financial statement assertions can be significantly affected by the clients use of an EDM system. This is discussed in Chapters 4, 5 and 6.
- Document authenticity is important in determining the nature of testing that will need to be performed. This is discussed in Chapters 5 and 6.
- The client becomes increasingly dependent on information technology to continue in business. This heightens the importance of general computer controls; this is discussed in Chapter 5.
- Traditional manual audit techniques, such as vouching, may no longer be available; however, more effective computer-assisted audit techniques may be available; this is discussed in Chapter 6.

Chapter 2

EDM TECHNOLOGIES

This chapter discusses the enabling technologies that facilitate an electronic document management system and discusses the six basic components of EDM.

ENABLING TECHNOLOGIES

As briefly addressed in Chapter 1, many recent technological advances in EDM can be attributed to the availability of more powerful processors at lower prices and wider bandwidths in telecommunications, making the technology more attractive to users. Meanwhile, advances in telecommunications and networking deliver higher volumes of documents on-line to the enterprise, increasing the pressure to manage them systematically. The expansion of document systems from LANs to wide-area networks enables enterprise-wide usage. These improvements in computing power and networking, along with the advances in software discussed in the paragraphs that follow, permit EDM systems to deliver value to businesses. This section will discuss some of the following technologies: 1

- authoring tools,
- imaging systems,
- optical character recognition (OCR) and intelligent character recognition (ICR),
- full-text retrieval systems,
- workflow systems,
- Internet and external computer networks,
- other technologies.

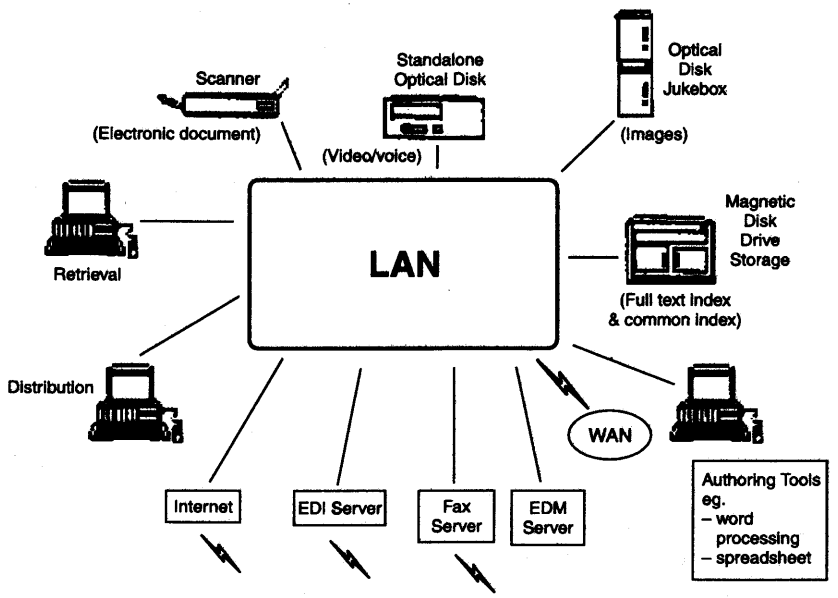
A diagram that identifies a number of the technologies is set out in Exhibit 1.

Authoring Tools

"Authoring tools" is a generic term used to describe any electronic package that can be used to generate an electronic document. The most common business authoring tools are word processors, spreadsheets, and graphic packages. In many situations, original documents will be created with these tools and passed to an EDM system, without ever being printed. 2

Exhibit 1

Electronic Document Management System Components



3 A properly designed EDM system's software will facilitate input and management from other desktop applications, for example:

- It should integrate with standard development tools, such as 4GL languages and prototyping tools.
- It should integrate with workflow systems.
- It should allow standard PC applications, standard database applications and peripheral services to be launched from standard graphical desktop environments.
- It should be able to operate on non-imaged documents or data kept in a file folder, such as forms, spreadsheets and word processing files and be open for incorporation into future multimedia objects like voice, pen and video.

Imaging Systems

4 Imaging systems capture documents using an electronic "scanner" device that transforms an original document into an electronic "image" representation. At the same time, "index" information is captured that helps identify the documents for retrieval purposes. Subsequently, the system transmits and routes images and associated data information to employee workstations for processing. The images are usually stored on large-capacity optical disks and can be retrieved and displayed on high-resolution monitors and printed on high-resolution laser printers. Fax machines can be used for both image capture and output. Although imaging systems may possess routing capabilities similar to workflow systems,

these capabilities may or may not be as flexible as those generally provided in workflow systems.

Imaging systems can be grouped into: 5

- *Low-speed file folder/workflow imaging systems.* These systems automate and replace current manual folder processing, such as loan and credit card applications, mortgage applications, and customer service.
- *Archival and retrieval systems.* These systems function only as simple storage and retrieval systems and generally replace microfilm/fiche.
- *High-speed image processing systems.* These systems are used for processing large volumes of identical images that require only minimal or brief human interaction. Most of these systems are used for remittance and check processing.

In 1991, the average cost of an imaging system was $600,000 for a *Fortune 1000* enterprise. The cost dropped to $200,000 in 1993, with a pilot project falling to less than $50,000. Costs have continued to decrease. The reason for these decreases is that imaging can now be done on more powerful microcomputers. The cost of integration and customization has remained static, however. 6

OCR/ICR

For certain types of applications, a key part of document scanning is optical character recognition (OCR). Printed text found within digitized images can be converted to Extended Binary Coded Decimal Interchange Code (EBCDIC) or American Standard Code for Information Interchange (ASCII) text by using optical character recognition (OCR) or intelligent character recognition (ICR). 7

Both OCR and ICR can be implemented in hardware or software. The hardware implementation may be considerably more expensive, but volume processing is significantly faster. Typically, high-end systems are expensive (about $20,000 or more), but they provide higher through-put rates and allow recognition to be done in the background without tying up workstations. Because of their low cost and flexibility, software systems have become popular in situations where high processing speeds are not required. 8

As previously mentioned, the typical conversion method still is scanning, but digital video and still-camera capture are becoming possibilities. These systems make use of data compression and decompression, another advancing area of technology. Refinements to OCR technology are enabling more of these captured images to be converted to hybrid text documents, which are easier to index. The improved reliability and accuracy of the character recognition technology has even made it possible to extend the OCR capability to recognize handwritten text; although the error rate when reading handwritten data remains high. 9

10 OCR software performs a number of steps to extract text from a digitized image:

- The software reads the bitmap (the matrix of pixels) created by the scanner and determines the white space on the page delineating, for example, headers, paragraphs, columns and graphics.
- The first step of conversion is based on an exact match between the pixels of a scanned-in character and the pixels of character sets stored in the program's files. Because an exact match is required, characters and attributes (such as bold and italic) may not be converted during this step.
- For characters remaining unconverted, the software analyzes features of the character, such as straight lines, curves and loops. The software builds an alphabet of characters based on the feature analysis and subsequently uses this alphabet to identify characters that could not be converted in the exact character match.
- Any characters remaining unconverted after this step are converted to a distinctive character, such as "@," so that a word processor can be used to manually search and replace unknown characters.
- Some OCR software packages also provide spell checking features to locate obvious errors and provide alternatives for words with unknown characters.
- The last step provides the option to save the converted image into ASCII or popular word processor formats.

11 ICR extends the functionality of OCR by implementing features such as omnifont recognition, which supports a wide variety of type fonts and hand-printed characters, and lexical analysis, which identifies characters based on the context in which they are used. A neural network-based engine can also be used for hand-print recognition. ICR is being used for full-text conversion in areas such as litigation support, where the entire contents of imaged documents are converted to text for subsequent access and retrieval by a text management system. The complexity of neural network technology requires a large number of computations; as a result, the applications are quite slow.

Full-Text Retrieval Systems

12 Text retrieval is the most widely used form of content-based retrieval document management. Text systems handle the creation, storage and retrieval of text. Text retrieval capabilities distinguish text management systems from other systems that create and store text, such as word processors. Text retrieval enables text to be searched on a variety of criteria including use of Boolean logic, QBF (query by forms), QBE (query by example) and, to a lesser extent, natural query language.

13 In a simple form, text retrieval is a document management system that references and retrieves structured or unstructured textual information based on words and word meanings found within the full content of the document. Text retrieval has no practical limit to the amount of text that can be stored in a document. Thus, it allows a single entry point to locating and retrieving all data pertaining to a potential query.

The link between imaging and text management systems is becoming stronger as the methods for manipulating image files allow for hybrid combinations of data, such as forms images overlaid with ASCII text. For all types of text documents, expert systems are being applied to aid in building indices and abstracts automatically. Search techniques are expected to dramatically improve with the addition of natural language interfaces, object-oriented query languages, ranked searches and special server-based accelerator boards. 14

Text retrieval is becoming a significant competitive tool for entities. Most industries have used text retrieval in some form. Most of the text retrieval systems are the base component of other applications since they can drastically alter the ability to work with large quantities of data in document form. Another strategic use of this technology is as a router of information. It often changes the entity from a distributorship model of information to a demand-based, user-centric model. 15

Various text retrieval architectures are available: 16

- *Stand-alone.* This is the most common architecture supported by text retrieval products. Stand-alone, PC-based text retrieval products are relatively inexpensive and now offer a range of features and capabilities that rival those in the networked and host-based arenas. The most prevalent drawbacks are:
  - limit to searching in a single document collection; and
  - low level of customizability — low-end products are typically integrated with a standard interface and metaphor that cannot be altered to any significant degree.

  If users need to access several such products for separate document collections, they will need to learn multiple interfaces and searching conventions. This can be a significant frustration.

- *Host-based.* Historically, text retrieval has been used most in the host-based environment. In a host-based system, multiple users can simultaneously access the document collection and query the system, but all of the documents must reside on a central platform. Furthermore, all processing and index creation is executed on the host machine. The end-user platform functions as a dumb terminal, whether it is physically one or not.

  Many text retrieval solutions continue to be used in a host-based environment. The market for systems has increased significantly, with desktop solutions expanding at a higher rate than mainframe solutions. As result, there are few new applications or installations in this area because there is an increasing trend to desktop solutions. What now remains is a large installed base of host-based users who are moving slowly to desktop solutions, predominantly in a networked architecture. The host-based applications that run on mainframes and departmental machines carry a much higher entry-level price. That is difficult to justify in all but the largest of text

retrieval applications. In contrast, desktop solutions can be scaled up as demand and sophistication of the users increase.

- *Networked.* Network-based text retrieval systems have become the most popular architecture for enterprise users. In a network scenario, users will access a single version of the document collection located on one node of the network and use the text retrieval engine on that same node to perform the search. Results are downloaded to the local node, where viewing and other operations, such as cut and paste, may occur.

Workflow Systems

17 There are two varieties of workflow systems: those that model workflows and those that automate and manage workflows. Workflow modelling tools take advantage of graphical user interfaces to plan workflow and envision revised business processes. These tools enable enterprises to examine and revise workflows prior to full-scale implementation in operational areas. Workflow software should provide a graphical management control tower where real-time workflow results can be viewed, modeled and modified. Control-tower viewing can be enabled from any PC workstation, given the proper security clearances.

18 Workflow automation or management systems automate standard procedures (for example, arranging mortgage financing) by imposing a set of rules on the procedure. Each task, when finished, automatically initiates the next logical step in the process until the entire procedure is completed. These systems can exert consistent controls over document processing or provide less formal controls to suit the needs of the operation and the criticality of the procedures. The application of expert system technology to workflow management systems is increasing the intelligence with which systems can route and retrieve information.

19 Workflow tools consist of job definition tools and advanced tools. The former are the means by which a workflow application is written. Their functionality can vary between products, but many contain at least some graphical tools to facilitate simple ad hoc workflow applications. These tools are limited in their ability to integrate complex applications. At the high end of job definition tools are highly transaction oriented workflow products used for customized applications (using graphical tools and 4GL scripting languages). Although powerful, they are difficult to use and require significant programming expertise and ongoing maintenance and support.

20 Most advanced authoring tools provide a high level of integration with other business systems and legacy applications. They are designed to facilitate customization of workflow applications. Again, although they range in functionality, most provide application program interfaces (APIs) but can also provide tools such as application program libraries, 4GL languages and integration with standard application development tools.

21 The distinction between workflow and document management software is often blurred, and the terms are often used interchangeably to describe

applications that manage the sharing of documents across multiple users and networked environments. Many workflow products do not offer a fully functional set of document management facilities, such as version control, content-based retrieval, security and audit trails. Despite the apparent synergy that exists between workflow and document management, the two sets of functions are not always in one product.

Internet and External Computer Networks

A popular transportation layer for network-based text retrieval is the Internet, 22
(and, for strictly internal purposes, an Intranet). These networks operate as described above for networked systems. With the increasing corporate use of Internet and other on-line computer networks, there is the potential to use such networks as direct inputs into an electronic document system. Because of the outside exposures, it is important to have strong computer access controls. Firewalls are being used more extensively to shield corporate computer systems from external networks.

Other Technologies (for example, fax, e-mail)

Other technologies that could serve as an inputs are discussed below. 23

Fax services and voice telecommunications

A growing application area for electronic document management is fax 24
integration to improve the speed of information distribution. Fax integration also provides capabilities such as annotation, conversion for editing by OCR devices, automatic filing by keywords and shared workgroup access. With the addition of voice telecommunications, EDM software can be coupled with a voice-response system for faxing stored documents (for example, in reply to common customer inquiries).

"Smart forms" is a new type of product that allows for remote data entry and 25
PC-based control. Typically, a form is faxed to a computer having a fax board and appropriate software that responds to commands set out in the form through a set of partially or fully filled-in shapes. By integrating fax machines as a primary input device, smart forms eliminate the need to rekey a large percentage of data.

One of the EDM system's growing applications is fax distribution. Facsimile 26
management software controls the sending and receiving of facsimiles to and from conventional fax machines. Some workflow automation software is capable of routing faxes throughout an entity. A growing number of systems employ a dedicated server processor to perform fax input/output.

E-mail

In an effort to lower costs and increase the use of EDM technology, a number of 27
vendors have begun offering software that image-enables standard Windows applications, such as databases, spreadsheets, word processing, and electronic mail. For example, one software package uses Microsoft's Object Linking and

Embedding (OLE) technology to integrate paper-based or fax-based documents with Windows applications. This functionality is especially useful in electronic mail applications; users can attach images of documents, such as contracts, résumés, invoices or correspondence, to their e-mail messages and route them to other users for review.

COMPONENTS OF EDM

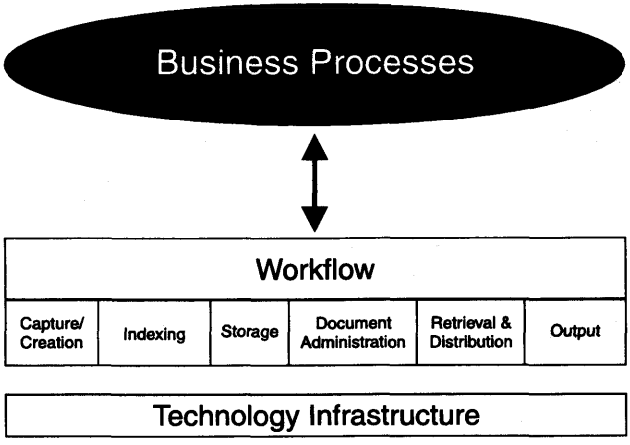
28 To understand the plethora of EDM technologies and products that an entity might employ, it is useful to identify functions or components. As illustrated in the following exhibit, EDM involves six basic components:

- capture/creation,
- indexing,
- storage,
- document administration,
- retrieval and distribution, and
- output.

The technologies described previously provide varying capabilities in each of these components.

Exhibit 2

EDM Components



Capture/Creation

29 There are three ways to capture/create documents:

- Creating an electronic document using an authoring tool and passing it to an EDM system for management.
- Paper-based information (for example, correspondence, forms, invoices, time sheets, contracts) is captured by digital scanning. This is a process in which a device similar to a fax machine reads the pages' light and dark areas and determines whether a given point on the page should be represented by a

black dot or a white dot. These dots — also know as pixels (picture elements) — are stored electronically as a bit-mapped image of the original page. This image can be retrieved and printed or displayed but, as an image, it is not editable text. An image cannot be pulled into word-processing software and changed unless it is captured and processed by an optical character recognition (OCR) system, in which case the image is transferred into text.

- Another method for capturing data is to receive electronic files over a communications network (for example, LAN, WAN, Internet etc.).

Scanning digitizes documents for manipulation and storage. Document 30
images are first divided into picture elements, or pixels, then each element is stored. There is a wide variety of scanners on the market, with an array of features to meet most scanning needs. Evaluation criteria for scanners include: compression algorithms implemented in hardware or software, throughput volume, speed, scanning resolution, single-sided vs. dual-sided sheetfeed options, and paper sizes (from business card to over-size engineering drawings).

A letter page that consumes almost one megabyte of storage in uncompressed 31
form can be compressed to 50 KB due to the large quantity of white space in most business documents. After scanning, a quality assurance (QA) process is performed to ensure that the entire document was captured in digital form and it is legible.

The capacities of both storage and networking subsystems are greatly 32
improved by compressing the captured data. Due to their large size, image files are stored and transmitted in compressed format. It varies with the image, but a typical compression ratio is 15:1. Typically, special-purpose hardware or software compresses the captured image data. To display or print the images, the compressed data must be first decompressed at the user's workstation or print server.

The ability to handle color images has been hampered by the inefficiency and 33
high cost of handling the associated large data volumes and the lack of standards. For a monotone (black and white) image, one bit represents the pixel color. For a color image, four to 32 bits may be used to represent the color of a pixel, significantly increasing the size of a color image. The emergence of compression industry standards for color images, primarily the Joint Photographic Experts Group (JPEG) standard, and MPEG for video, has made handling color images more economically feasible.

Indexing

After the document is captured/created and verified, it must be indexed. Indexing 34
involves entering character data that describe or tag an image for subsequent retrieval. This data can range from serial numbering to a lengthy, structured description. Traditionally, these data are entered manually from the keyboard. In the case of scanned image documents, the development of more sophisticated scanners has reduced manual indexing by using OCR to recognize characters from specific zoned areas or bar codes scanned from the document. Intelligent

scanners can, in fact, create an index. As a result, options for indexing scanned images can include:

- manually entering indexes with one or more fields;
- coding, for example, bar or scattered dot coding;
- designing special forms for automatic assignment to file folders; and
- using intelligent scanners and optical character recognition of pre-specified fields to build the index. Key information, account numbers, form numbers, words or phrases can be stored and subsequently used to locate and retrieve images.

35 In the case of electronically created documents, EDM systems can provide standard templates for the most commonly indexed documents, reducing user input and error potential. Combined with workflow software, these templates may even be pre-selected, depending on where the user is in a workflow sequence.

36 Indexing data are stored in a database that is separate from the actual documents. The type of data that can be used to retrieve a document is a function of the index database. Some allow the document transaction history to be recorded. Other index databases link the document files to existing databases from other applications by pointers or common fields. EDM systems may not need to provide index management services if an existing database can search for documents by attributes, such as an applicant's name or social security number. For example, a social insurance/security number can be assigned as a document locator number during capture/creation. Then, the existing database can be used, say, to search for all documents that pertain to a particular region by the social security numbers of all applicants that live within a certain state or zip/postal code area.

Storage

37 The third component of an EDM system is storage. Two factors influence the choice of storage media for EDM systems: how long the documents need to be stored and how often they are to be retrieved. EDM systems generally use some form of hierarchical storage manager (HSM) to deal with the varying demands of in-process and archival document stores. In-process documents are normally stored on magnetic disks, whereas archival documents may (particularly in the case of scanned images) be stored on an optical media.

38 Four types of storage can be used in an EDM system: magnetic, optical, microforms, and hybrid. Each of these storage options is discussed below.

Magnetic media

39 Magnetic media for EDM systems include conventional hard disk storage, redundant arrays of inexpensive discs (RAID) technology and digital audio tape (DAT). Large hard disk drives are being used in small systems as local repositories for documents to reduce the load on the network and to improve system response time. The cost per megabyte is higher than with other storage

alternatives, but it can be used to avoid the introduction of new technologies or to supplement optical media in highly distributed systems.

Formerly, magnetic media stored only electronically authored documents and cached or pre-fetched images. This improved document retrieval times and flip rates (the rate at which subsequent images can be brought to screen after the first has been viewed). With the advances in RAID technology, magnetic media are becoming a viable storage option for medium and large-scale imaging systems. With products such as high-capacity drives, magnetic media can be viable as a primary storage option for imaging systems. 40

Digital Audio Tape (DAT) can hold approximately 1.5 GB and is used in EDM systems primarily as a back up medium and as a master for CD-ROM. Multiple DAT cassette loaders that store approximately 10 GB are available. A bulk erase utility is employed for tape re-use. 41

Optical storage

Optical discs provide high-density storage at significant cost savings per megabyte over magnetic media. Recent advances in optical storage and jukebox technologies have paved the way for widespread acceptance of imaging technology. Optical storage for EDM systems includes Write-Once-Read-Many (WORM), magneto-optical, CD-ROM, optical tape and Computer Output to Laser Disc (COLD). 42

WORM provides high-capacity storage that can be written to but that cannot be erased. It is an excellent archival medium. An index to the WORM drive is usually stored on magnetic media for continual updating. When records are no longer needed, the index to those records can be deleted. 43

Magneto-optical is a rewritable medium that provides the high density storage of optical media with the revision capabilities of magnetic media. Increasingly, magneto-optical is being implemented in large-scale systems for storing both work-in-process and final documents. 44

CD-ROM is a fixed optical medium that requires data to be formatted and pressed on to a CD. Formerly, tapes of pre-formatted data were sent to production facilities for pressing. Recent advances in CD-ROM technology, however, enable user entities to press their own CD-ROMs and even append files to them at a later date. 45

Optical tape is a very high capacity WORM technology medium used primarily for EDM system back up. A library of 16 tapes can store very large volumes of data, up to five pentabytes (PB). 46

Computer Output to Laser Disc (COLD) can be used to capture voluminous computer output reports on-line as ASCII text. Rather than printing case upon case of computer reports in multiple formats, COLD stores a template for the text, and merges the template with the text for presentation to the user on an ad-hoc basis. 47

Microforms

48 Microforms include film, fiche, aperture cards and computer output to microfilm (COM). Companies that require frequent access to archived documents or have limited storage space often store documents on microfilm. Banks, for example, use microfilm extensively in check processing. One disadvantage of microfilm is that it records documents serially and, consequently, it can be time consuming to retrieve a particular image. Computer-Assisted Retrieval (CR) can be used to automatically retrieve filmed images using an electromechanical arm that fetches the correct roll of film, loads it on to a reader and advances to the correct frame.

49 Unlike microfilm, microfiche storage provides distinct sheets of filmed images, which can be accessed directly after searching the index. Microfiche is used extensively for price lists, product listings and library card catalogues, among others. Individual fiche can be updated and redistributed cost-effectively.

50 Computer-based information can be output directly on to microfilm using computer output to microfilm (COM). A COM recorder generally consists of a narrow cathode ray tube (CRT) that displays the computer output one line at a time. The film is in contact with the tube and moves past it in synchronization with the display. COM is a fast and efficient way to store documents.

Hybrid storage

51 As enterprises migrate from existing storage devices to selected new components and technologies, a hybrid storage strategy often emerges. Some entities will define schedules for retaining records and target storage media for each class of records, and then retain a hybrid storage structure indefinitely. Others will migrate toward the new storage system to the exclusion of the old. Most storage migration decisions are made after a cost-benefit analysis based on the cost to retrieve information, the expected frequency of retrieval and the likely consequences of the inability to retrieve information when needed.

52 For documents that must be stored over long periods, microfilm or optical storage (sometimes referred to as a laser disk because the information is written to and read from the disk using a laser beam) is preferred over magnetic storage. Magnetic storage is useful in applications that require a high retrieval rate but are relatively low in volume. Optical storage is usually recommended for high-volume, high-retrieval rate environments. The choice of rewritable versus write-once (WORM) optical disks depends on the applications requirements for ensuring the preservation of the original document over time.

53 While image data can be stored on magnetic media, optical disks are the technology of choice because of their high capacity for secure data storage. Digital image files are large: a single page requires 50,000 bytes of storage, and optical disks typically can store from 40,000 to 150,000 of these pages each. Most optical disks used in image processing fall into the Write-Once Read-Many category. These files cannot be erased or changed. Experts once thought erasable optical media were essential to the growth of the image market; despite the ready

availability of erasable optical media, however, WORM storage is far more prevalent.

When considering the use of optical media for long-term storage, it should be remembered that optical disk storage has not been proven equal to archived microfilm for longevity. This shortcoming of optical disk storage can be overcome through periodic backups or a records management procedure that coordinates optical disk storage with paper and film. In the latter case, the EDM index database is used to keep track of all media. In addition, the entity needs to ensure that it will always have the appropriate hardware that will allow it to read the optical disk. With the current pace of technological changes, the availability of compatible hardware could become more problematic than the issue of longevity of optical disk as a media for storage. 54

Document Administration

A number of issues need to be addressed in document administration, including: 55

- document modification and version control;
- retention, archiving and back-up policies;
- contingency planning and disaster recovery;
- records management.

Document modification and version control

Version control is an important safeguard that provides evidence as to document modification (authorized and, potentially, unauthorized). To facilitate this control, the index information should contain complete bibliographic information for locating and retrieving documents: 56

- author or source of the document;
- exact date of capture/creation;
- capture device location;
- any details on modifications that have taken place; and
- appropriate cross-referencing information.

Scanned images can present special version control issues. Captured images can be manipulated to create new documents. Three methods are typically used to manipulate images to create new documents: 57

- Image combining — A new document is created by combining images from different documents and associating a unique index to the new combination. This method does not alter the stored images.
- Annotation — The annotation function modifies the image view by producing an overlay (mask) which is linked, in the database storing the image record, to the image. Users can view and print the image with or without the overlay. This method also does not alter the stored images. Annotation is particularly suited to provide electronic red lining, "post it" style of notation and margin editing functions in imaging systems.
- Raster editing — Images can be modified, using a raster editor, to create new ones. A raster editor changes the image pixels. Raster editing alters a stored

image. The original image may or may not be preserved by raster editing a copy of the image.

Retention, archiving and back-up policies

58 EDM can dramatically expand an entity's reliance on its information systems. In addition, the volume of data that needs to be backed up is significantly larger due to the size of images.

59 The entity should back up all data systems on a regular basis. Back-up media should ideally be stored at a physically secure off-site location apart from the entity's main system.[1] Back-up copies should be generated for all system software and, on a daily basis, computer-coded data (especially the database index). This back up is typically done using high-capacity media, such as optical disk or high-density magnetic tape. Because of the length of time required to write the data back up, the copy is often made either simultaneously with the primary disk or in an automated mode during off-shift hours.

60 Implementing adequate back-up recovery plans for document management systems should not differ drastically from traditional computer system recovery plans, although EDM systems often require high-density media to store large image files. The following should be considered when developing recovery plans involving image systems:

- While optical media are more durable than traditional magnetic storage technology, they are not indestructible. Failing to recognize this when designing back-up and disaster recovery procedures could cause significant problems;
- While image files are usually stored optically, the index is typically stored on more vulnerable magnetic disk devices. The back up and recovery of both index and image files need to be coordinated.

Contingency planning and disaster recovery

61 One of the keys for survival is to have adequate data back up and to have an appropriate disaster recovery plan in place to allow the entity to continue in business should a disaster occur. Involved in the contingency plan would be:

- recovery plans for new devices and networks;
- arrangements for alternative processing sites;
- effect of recovery on document integrity certification;
- ability, if possible, to function manually while recovery arrangements are activated.

62 Persons responsible for bringing the EDM system back online, in the case of a disaster, need to establish detailed procedures for each step of the recovery and

---

[1] It should be noted that the SEC requires brokers/dealers who rely heavily on optical storage systems to have duplicate, off-site storage facilities.

ensure that the computer equipment necessary to effect the recovery will be available, if needed. The client should test this plan periodically to ensure that it will work effectively.

Records management

The mere scanning of documents is not records management. A sound records management program should satisfy diverse requirements: 63

- functional and operational needs should be met;
- the entity's history needs to be preserved;
- vital interests need to be protected;
- the data should comply with confidentiality and privacy policies of the entity;
- technological compliance needs to be maintained, that is, the entity needs to be able to recreate the environment that created the archive, otherwise it may not be able to retrieve it;
- records need to demonstrate regulatory compliance and ensure that legal status is maintained.

Variations in the way that records are retrieved and used for different functions frequently waste time and resources. Common inefficiencies include duplication of documents, records maintained too long, inappropriate indexing and lost documents. EDM can reduce these problems as long as a sound records management process is in place, one that exercises control over the creation, use and disposal of records (or, in the case of CD-ROM or optical records, which are de-indexed). Also, program supervisors should have a detailed knowledge of the records program theory, history and practice, to know whether objectives, policies and documentation are being carried out. 64

Some legal considerations for electronic documentation are discussed in Chapter 5 and Appendix B. 65

Retrieval and Distribution

Document retrieval is primarily a character-based function. Users search on key words or numbers to find documents and related information. The retrieval and distribution components of an EDM system include software for locating the stored document, and hardware to display or print the document. The retrieval software uses an index created using a database that stores information about the document. In an insurance system, for example, index information might include policy number (a link to existing systems), type of document stored and the document's location (a link between the database record and corresponding document file). To increase access speeds, the document index database is often stored on magnetic disk, apart from the documents. The index database may also be stored on a separate dedicated server or on a host mainframe, apart from the EDM system. 66

The capture, storage, retrieval and distribution components are linked into an image-processing system using microcomputers, minicomputers or mainframes, depending on the size and complexity of the system. 67

Data Output

68 Data output alternatives include printing documents and transmitting electronic files.

69 Once the desired document is located, it can be viewed at a display station (typically an industry standard PC, possibly with a special monitor) and/or printed on a laser printer. Increasingly, fax machines are being used for remote distribution. Most commercial laser printers can print corporate documents and images along with character data. In LAN configurations, data decompression is usually performed at the printer to reduce the burden on the network. To accommodate the large number of pixels per page (10 times more than that needed for displaying images), printers are often connected to dedicated PCs acting as print servers that can be shared by all users on the network.

Chapter 3

BENEFITS, RISKS AND PRE-IMPLEMENTATION CONSIDERATIONS

This chapter discusses the benefits and risks that can be attributed to the use of EDM and deals with important pre-implementation considerations, including the benefits of auditor involvement.

BENEFITS

Summary

Entities with effective document management systems should capture, retrieve and process information more efficiently, resulting in higher quality, more timely, and lower cost service to the customer. The greatest benefits of document management should go to entities that optimize business processes, then match the document management systems to those processes. Entities that do not use such systems will likely face increasing competitive pressures from those that do. 1

Intelligent document management systems should help workers deal with the wide variety of documents arriving at their offices. At their best, these systems should provide one simple access point for e-mail, bulletin boards, periodicals, fax, voice mail, forms data, business transaction records, such as purchase orders, and remote databases. The workflow component of these systems should help people process and dispense with documents of all sorts. Activities such as routing, distributing, rejecting and filing documents should be automated. 2

In some cases, interest in EDM systems will stem from the desire to streamline interdepartmental or interorganizational work. This can lead to overall business process reengineering and have far-reaching effects on the enterprise. For example, if interdepartmental cooperation eliminates the need for certain types of documentation, the cost of the business process is reduced. 3

The use of EDM should produce a significant cost savings for the participating entities. As long as the technology is properly implemented with adequate controls, EDM offers several advantages over manual, paper-based systems. These are discussed in the paragraphs that follow. 4

Reduced Storage Costs

5 Most businesses do not realize how expensive the storage and retrieval of paper documents are. Not only are the original documents created but, frequently, copies of these documents are made and the entity has to store the same document several times. Entities with branch offices may often store a copy of each document in each office.

6 It has been estimated that the cost of owning and maintaining a standard five-drawer file cabinet is $880 annually, with the annual cost-per-filing-inch being $11. At $20 per sq. ft., 50 such drawers — roughly equivalent to the space of a 16 ft. by 24 ft. room — would cost the entity $50,000 per year to maintain and would occupy several employees. Conversely, a 12-inch optical disk holds images of approximately 100,000 business letters, equivalent to 50 filing drawers. The cost of an optical disk is a fraction of that needed for paper filing, and the system can be run by far fewer people. For example, one financial services company decided to invest in imaging technology. After six months the company had disposed of nearly five tons of paper records and reduced its archive space by 60%.[1]

Enabling Simultaneous Retrieval

7 EDM enables retrieval and display of any available file from any authorized workstation or user in the system and, enables employees at multiple workstation locations to simultaneously retrieve the same document(s). This allows them to complete their assignments simultaneously, rather than sequentially. This electronic transfer and concurrent sharing of information significantly accelerates business processes that require multiple stages and multiple sources of information.

Enabling More Accurate Data Entry

8 Data entry errors are normally the most frequently encountered errors in an information system. A properly controlled EDM system significantly reduces these errors because data re-keying is replaced by electronic scanning; this is far more accurate. As a result, errors and error correction costs are reduced.

Improved Productivity

9 Entities that have installed EDM systems have noted productivity gains from 20% to 50%. These gains have allowed entities to trim their clerical staffing requirements while increasing capacity.

10 Workflow can also be impaired by misfiled or lost paper. It has been estimated that, at any time, 30% of an entity's paper files/contents are misfiled or in use. This problem, common in paper-based systems, can result in increased

---

[1] Example cited in *Audit and Control Issues of Image Processing* Computer Audit Update (Elsevier Science Publishers, March 1992), p. 16.

liability, loss of loan insurance or loss of customers. It has also been estimated that executives spend more than 150 hours annually looking for information that was misplaced, misfiled or missing, with the average cost of each misfile being $120. One of the most significant benefits of EDM is the avoidance of lost or misplaced files.

In the financial services sector, the number of products and services offered are increasing in complexity, yet the number of skilled workers available in the marketplace is decreasing. By using EDM, entities can meet their new product requirements with a smaller number of staff. 11

Reduced Time for Search and Retrieval and Reduced Document Loss

The time spent accessing paper documents is one of the biggest hindrances to getting work done. One of the major impacts of EDM in any paper-intensive industry is the significant reduction in the amount of paper documents being handled. Jobs that previously took weeks of searching through paper files can take just minutes at a keyboard and a screen. 12

Better Management of Consistent Processes

EDM is beneficial in environments using production or transaction-oriented work management. This type of work requires personnel to perform repetitive tasks in which documents may need on-demand access days, months or even years later. Throughout, policies and practices are needed to create and maintain an audit trail for each document. Examples of these types of business include transportation bills of lading, medical records, engineering project management, credit-card processing and correspondence, insurance claims processing, mortgage loan processing and insurance underwriting. 13

EDM can greatly assist with processing customer-initiated, document-based transactions. For example, images of insurance claim documentation can be stored on-line and transmitted with the claim as it moves throughout the entity. EDM helps route the claim through the approval process. 14

There are also many uses for EDM outside the financial services sector. Accounts payable invoices can be routed through the requisite approval and subsequent payment process by EDM. The data in the purchase order can be stored with the image of the signature for recall anywhere on a network. Also, images of the approved invoice can be stored on-line and retrieved by the computer as evidence for approval and payment. 15

Improved Control Through Complex Administrative and Other Processes

EDM has been found to be beneficial in complex industries, such as defense and automotive. The US Department of Defense is promoting computer-aided acquisition and logistics-support-compliant document-management systems. Auto manufacturers are using on-line, full-text retrieval systems for looking up rules and specifications in lengthy design or regulatory guides, using expert 16

systems to access relevant guidelines. Engineering drawings are stored on line in hybrid data bases along with approval information and explanatory text.

Preventing Unauthorized Access to Documents

17 By controlling documents through EDM, managers control not only the manner in which documents are linked with other forms of information and applications, but also how they are distributed or accessed by staff. EDM allows information to be accessed at each employee's workstation by authorized employees only.

Increased Control, Security and Disaster Recovery

18 EDM systems provide a complete, secure and controlled store of all of an entity's information. Using prudent offsite and hot-site arrangements, an entity can protect itself from significant loss.

19 Exhibit 1 sets out some examples of savings that have been achieved through the use of EDM.

Exhibit 1

Examples of Cost Savings

An oil producing company, in 1993, became significantly larger due to a new field that caused not only a significant generation of oil but of paper; a 75% increase in the invoices, requisition forms, commitment forms, and so on. Due to EDM, the 75% increase was handled by existing staff.

A telephone company using EDM cut costs by 80% and saved $750,000 on every product release.

A manufacturer using EDM improved overall productivity 20 fold and increased time savings by 25% to 50%.

A bank reduced microfilm expenses by more than $750,000, has less staff requirements, increased productivity and now has 100% file integrity. In the first six months, its imaging system saved $1,000,000 more than it cost.

A large mutual fund company introduced EDM. Projected costs savings are 30% per year and a payback period of less than two years is expected.

RISKS

20 Poorly managed systems may inadvertently add new inconveniences as they may further complicate or restrict the process of retrieving documents. Perhaps worse, they may introduce cumbersome procedures that were unthinkable in manual document handling and hard to manage even electronically. System failures prevent access to all documents. Controls over EDM processing should be designed in the context of the entire information management system. EDM-based information is only as secure as the rest of the system.

Total Systems Dependence/Business Interruption

Business interruption deals with risks that interfere with the ongoing operation of an enterprise. As document management systems increasingly support mission-critical business processes, the risk of business interruption due to loss of data processing increases. This is one of the greatest exposures a client incurs with an EDM system. Paper documents, which were relied on as a source of back-up information, may not be available. Consider, for example, the impact on a credit card processing company or on an insurance claims processing operation if the EDM-processing system becomes unavailable. System redundancy, disaster recovery and controls techniques designed to minimize the risk of such occurrences should be implemented. 21

Data Processing and Application Errors

Error, the most common control risk, places an enterprise in a situation where business decisions or judgments may be made based on wrong information. Programming bugs, inadvertent indexing, scanning errors and the quality of the data itself need to be controlled to reduce such risks. 22

Inaccurate Capture of Information by the Document Management System

Document management systems have introduced new ways for capturing data (direct transfer of electronically authored documents, scanning, OCR, ICR). If appropriate data capture controls are not in place, the accuracy of the information in the system could be jeopardized. Traditional, proven data entry controls must be used in creating the index database, and new controls must be developed to assure the legibility of documents read through digital scanning, ICR and OCR. 23

Concentration of Control

The strength of internal control offered by segregation of duties and structured management reporting may be reduced or weakened in an EDM environment because fewer people now do the work. EDM places a greater reliance on computer systems and concentrates control in the hands of fewer individuals, with the potential to increase risk. While effective automated controls could reduce the potential for human error, the impact of any control deficiencies could be greater. 24

Potential Loss of Audit Trails

This is addressed in Chapter 4. There may be less paper available for verifying and reconciling transactions. There is also a concern that, without proper controls, data can be lost. 25

Potential Inadmissibility of Electronic Evidence

The use of imaging as an information medium is important because of the benefits it offers. There are numerous instances, however, where imaging is not being used to its full potential because of the uncertainty of whether the resulting images may be admitted into evidence in court proceedings. No law prevents an 26

entity from copying its own records if it keeps the source records. Rather, the issue is whether an image-produced record will be credible and admissible in court when its source record has been disposed of. The client needs to implement proper controls to ensure that the electronic records are deemed legal. This is discussed in more detail in Chapter 4 and Appendix B.

Increased Reliance on Technical Resources

27 As document storage moves from paper to electronic media, the problems of storing paper should shift to the problems of managing databases. Rather than leasing space to warehouse voluminous paper files, entities will need to maintain sensitive electronic equipment. This should change the amount and type of floor space required, as well as the location of files and storage.

28 An entity's employees need to understand task processes before they can productively use EDM or other electronic information systems. EDM can have an impact on the skill sets required. It changes the skills required to manage the storage; for example, instead of administrative assistants, the entity will need computer network and database administrators. The creation of procedures and the use of training is important in helping staff effectively use these new tools. Staff need to understand the tasks related to the critical application processes to effectively use them.

Unauthorized Access to Systems

29 It is important to have controls ensuring only authorized users have access to document management systems. Paper documents are secured through physical measures such as storage in locked vaults. Electronic images are secured through logical access controls to ensure they are not read or altered by unauthorized individuals. In addition, there need to be appropriate access controls surrounding documents, indexes, annotations and text files to prevent unauthorized changes or deletions. This is discussed in more detail in Chapter 5.

Fraud

30 The risk of fraud — criminal conduct aimed at intentionally altering, destroying or counterfeiting documents — increases if access controls and management trails are not adequately maintained, monitored and enforced. Controls, such as those set out in Exhibit 2, should be considered.

Lack of Compliance with Regulations or Standards

31 Some entities must comply with regulations and industry standards. If the form of record keeping is changed, there could be a risk of not complying with such regulations or standards. In the consumer loan environment in the US, for example, signed agreements and titles must be kept and stored off site in a secure environment, while correspondence, credit reports and the loan application itself can be destroyed after scanning.

32 Compliance also involves adherence to standards. While EDM standards remain somewhat *de facto* in nature, a number of entities, such as Association

for Information and Image Management (AIIM) and the Department of Defense, the Canadian General Standards Board, have established guidelines with which image-processing systems may have to comply.

PRE-IMPLEMENTATION CONSIDERATIONS

Three areas need special attention when an entity is planning to implement an EDM system. The first relates to assessing the business opportunities for using EDM and its potential benefits. The second relates to developing and using a project plan to manage the implementation and monitoring of all the applications, once they are established. The third relates to proper controls, that is, the entity needs to design and implement appropriate controls and supporting working practices to address the risks associated with EDM. 33

Need for Client EDM Program

Records managers and others who are using or are contemplating the use of EDM should have a proper EDM program in place to ensure that evidentiary requirements are met and that adequate controls are in place. Some of the issues that should be covered in that program include: 34

- Proper documentation — All procedures and systems involved in the capture, storage, retrieval and processing of EDM transactions should be documented in a comprehensive procedures manual. The manual is the entity's authoritative standard and can be a persuasive piece of evidence if it is written before any litigation issues arise (notably, before incentives to falsely documents in a system arise). The manual is to be generally available and should be used by all staff involved in the EDM program.
- Executive endorsement — The program should be endorsed, in writing, by the entity's management. The endorsement should clearly cover the use of the procedures and systems described in the procedures manual.
- Integration into the normal course of business — The procedures and systems that comprise the program of records capture, storage, retrieval and fraud prevention should be fully integrated into the entity's normal and ordinary course of business. Examples of evidence of this integration might be the inclusion of EDM-related functions within job descriptions and the inclusion of capture and retrieval statistics in the regular management reports circulated in the business area.
- Documented authority for destruction of the originals — To establish the credibility of the EDM record, the original record should be destroyed in a controlled and authorized manner. There should be documented authority by responsible officials for the regular destruction of the originals, and the prescribed program of destruction must be followed. This should involve a sign-off by all of the key players involving functions such as accounting, technology, the business unit and the legal department. Deviations from the program, if not documented, may cast doubt on the status of all images as having been made in the normal course of business.
- Quality assurance as part of the program — A comprehensive system of quality assurance should be built into the EDM program. Quality assurance

activities should be in evidence to address the completeness of capture of all records received by the entity, the accuracy of capture of individual EDM transactions, the completeness of capture of all relevant features of a business record on the transaction, the authorization for the capturing of the business record, and the maintenance and preservation in unaltered form of the captured transaction. This last point implies that the use of a "non-alterable" medium may be required to persuade a court that records have not been altered. It may also be important to monitor and tightly control any capability to alter transactions between the time they are captured and the time they are written to the "non-alterable" storage medium.

- Proper storage and preservation of the media — The EDM program should provide for the proper safeguarding of the media on which the transactions are stored. Ideally, entities should maintain at least two copies of any individual document, at least one of which is on a non-alterable medium that does not deteriorate. Procedures and/or systems must be in place that should provide assurance that operational copies maintained on alterable media are equivalent to the non-alterable archival copies.
- Conformity to applicable standards — The technological means for capturing, storing and retrieving the EDM transactions should be generally accepted as a widely used standard. This does not preclude the use of technologies where a *de facto* standard exists, but has not been endorsed by any standards body, nor the use of widely used proprietary methods.

35 These guidelines for an EDM program are a logical extension of standard procedures for records management and computer processing. Therefore, an entity that goes about its program in a logical, controlled, authorized and documented manner is likely to conform to the standard.

Backfile Conversion Considerations

36 One of the first steps for planning an EDM system is to determine which documents need to be converted. Besides the decision on which documents to convert on a carryforward basis, a decision on whether to convert an entity's backfile of documents also needs to be made. Controls for converting the backfile should differ from the controls associated with the carry-forward conversion process. Backfile conversion can add significant costs to implementing an EDM system.

37 When planning to convert from paper to another medium (in this case, to electronic image data on optical disks), the client has two choices: do it in house or hire a conversion specialist. Each approach has advantages and disadvantages, depending on the situation and requirements. Sometimes, a combination is warranted. In either situation, the client will want to ensure that:

- appropriate controls are in place to detect input errors;
- appropriate correction and clarification procedures are in place (including controlled re-scanning) to ensure that the data are clean.

In-house conversion

If the entity converts its own records, it may want to lease or purchase the scanning equipment best suited for its record collection. Scanning in house provides a level of security and control that is unattainable when working with contractors from outside of the entity. Reasons to scan in house, using the entity's own employees, include the following: 38

- documents are content sensitive or classified;
- documents (existing, new or both) are in such high demand that they should not leave the facility; and
- scanners purchased for new documents entering the system may be idle for substantial work periods and the backfile can be converted slowly during those times.

It may be more expensive for the entity to scan documents than to have conversion contractors do the work. Unfortunately, scanning is a skill that improves as an operator gains experience. Many document collections are of such a size that the backfile conversion is completed at about the same time scanning operators gain enough experience to really be effective. In addition, the equipment required to perform the backfile conversion may be far more expensive than that needed for the ongoing EDM operation. 39

Service bureaus

As specialists, service bureaus are in the business of document conversion; they often have years of management experience. They offer well-trained operators with experience in converting a variety of document types to many different media. Most service bureau operators are bonded; some have security clearances for handling sensitive documents. Conversion costs from a service bureau may be less than if the entity purchases equipment and hires and trains operators. 40

In any event, it is important for the entity to discuss its scanning requirements with vendors, systems integrators, and service bureaus. They should be made aware of document quantities and characteristics, the timetable, the work shifts available, any staffing considerations, and other special circumstances that may affect the conversion. 41

Other issues that need to be addressed include: 42

- What procedures will be in place to ensure that the documents are properly identified when they are received?
- How soon after it receives new paper documents will the entity need to retrieve them in either paper or electronic form?
- What procedures are in place to ensure accuracy and completeness of conversion?
- How active is the backfile collection?
- What media (other than paper) will be converted?

Retaining original records

43 The client should address whether it or its service bureau should keep the original source documents. This involves considering the legal, operational, and statutory implications of disposing of records. Although destroying original records eliminates the expense of refiling and storing the paper, the records must be kept if specifically mandated or if authenticity or certification is required. If records must be kept for long periods, will the optical media, disk reading device and/or operating software be durable enough to service? In these cases, the entity may want to either keep the original document or convert the records to a durable medium, such as microforms.

Auditor Involvement

44 Entities and their auditors can reap significant benefits from a properly implemented and controlled EDM system. In general, an entity's management that wants assurance that the conversion to EDM is complete and accurate should consider involving an auditor with the required technical expertise at an early stage in the conversion process. Although not a requirement of generally accepted auditing standards, it is beneficial for the auditor to be involved as soon as possible in the EDM development process, in order to assess what controls are to be included in the system and to plan how the system could be used to help in the audit. In order to obtain the benefits, the auditor should:

- understand the technology;
- consider an active involvement in development phases of an EDM system to ensure that the client considers all necessary control requirements including, for example, proper segregation of duties and controls surrounding the capture of images and text;
- test, if possible, the backfile conversion, that is, the conversion of part or all existing paper records into electronic images before the system goes live. This not only represents a significant effort, but also requires controls in the same manner as the production system to ensure authenticity and quality of electronic images;
- assess the back up and recoverability of the data in case of interruption;
- ensure that data security controls are in place;
- ensure that appropriate data are available for audit purposes.

45 While obtaining evidence that appropriate controls are designed into an EDM system at an early stage, the auditor can prepare to directly benefit from the technology's capabilities.

46 Exhibit 2 sets out some of the key control issues that an entity may need to face.

Exhibit 2

Some Key Control Issues for Entities Using EDM

Areas of Risk	*Control and Purpose*
Error	Automatic document recognition controls to prevent duplication of capture Automatic indexing to ensure that a document is linked to adequate and correct indices Control activities[2] to detect, report and correct errors on a timely basis Internal auditors to regularly review EDM system security and controls Training to develop a proper understanding of the EDM system
Confidentiality & Disclosure	Confidentiality policy for document classification Network security to deny access to unauthorized persons Index and document controls to prevent unauthorized security disclosure through the use of index and document searches for key words Encryption software to protect confidential sections of documents Output device restrictions to prevent reprinting of confidential documents
Business Disruption	Contingency plan for backup hardware and software to minimize business
Vandalism	Physical security in areas where EDM equipment is located and original
Fraud	Manual authentication and verification procedures to ensure input is restricted to authorized documents only Audit trails and control reports to identify amendment of documents and unauthorized printing of documents User access controls to segregate incompatible functions while still allowing staff to deal with more facets of customer processing Manual verification procedure to ensure completeness of capture/creation.

[2] Statement on Auditing Standards No. 78 *Consideration of Internal Control in a Financial Statement Audit: An Amendment of SAS No. 55* (N.Y., N.Y.: AICPA, December 1995), p.17, defines control activities as "the policies and procedures that help ensure that necessary actions are taken to address risks to achievement of the entity's objectives. Control activities have various objectives and are applied at various organizational and functional levels".

Chapter 4

AUDIT PLANNING ISSUES

This chapter deals with planning issues for auditing an entity using EDM. Chapter 5 addresses, in general, the controls that may be found in an EDM installation and the related audit implications and possible audit techniques.

PLANNING ISSUES

Assess Impact of the EDM System and the Form of Audit Evidence

The first issue an auditor should consider is the impact of the EDM system on the financial transaction system. As set out in Chapter 1, the EDM system may have direct impact, indirect impact or no impact at all on financial transaction systems. 1

Also, the auditor could have two additional considerations in respect of the audit evidence that an EDM system has available: 2

- Where documents still exist in paper form, the auditor may want to ignore the EDM system and just use the paper audit trail, if desired. This would not, however, preclude the auditor from testing controls.
- Where no paper is kept, the auditor may need to consider testing controls in the EDM system to ascertain that the data supplied to or supporting the transaction system are; for example, accurate, authorized and timely.

Where there is a direct-impact system, it would likely be more effective and efficient to test controls and then use the EDM system to produce the background audit evidence supporting the financial transaction. In an indirect-impact system, the auditor would use either paper or electronic evidence, depending on the circumstances. This is discussed fully in the audit approach set out in Chapter 6. 3

As briefly addressed in Chapter 1, the issue of "document authenticity" is key. To use computer-based auditing procedures effectively, it is important that the auditor is satisfied that the EDM system contains complete and accurate information. These issues are discussed in paragraphs 44 and 45 of Chapter 5. If the auditor is satisfied that all data in the EDM system agree with the original documents they were captured from and that proper version control is exercised, 4

then the EDM system itself can be used to greatly facilitate the audit. This is discussed in more detail in Chapter 6.

5 The auditor needs to be able to develop procedures that will be effective and efficient in the particular circumstances encountered. Traditional audit techniques, however, may not be effective. There will be the potential to use computer-assisted audit techniques, however, to extract appropriate data from the EDM system to obtain audit evidence regarding the financial assertions (see Chapter 6).

Use of a Specialist

6 It is important that the auditor have the appropriate knowledge and skills to audit an EDM system. If the auditor does not have skills to audit complex computer systems, it may be necessary to use a specialist to provide assistance in gaining an understanding of the EDM system and to help the auditor design appropriate audit tests. In these instances, the auditor should be guided by the guidance set out in the professional standards of each country.[1]

Knowledge of the Business

7 The need to have sufficient knowledge of the business is fundamental to planning and executing audit procedures and evaluating the results of those procedures. Obtaining a knowledge of the client's business assists the auditor in a number of areas, including:

- identifying the nature and source of audit evidence available;
- identifying areas that may require special consideration;
- assessing conditions under which accounting data are produced, processed, reviewed and accumulated;
- evaluating the reasonableness of management representations;
- evaluating the sufficiency and completeness of the audit evidence obtained.[2]

8 When obtaining a sufficient understanding of internal control to plan the audit, the auditor would consider matters such as the relative complexity of the client's information systems, as this would be pertinent to the preliminary assessment of control risk. The use of EDM and the resulting impact on client business practices, including those affecting financial reporting, can vary significantly among entities. In many cases, the entity is simply receiving invoices in a different form. Clerical control activities may still operate effectively, and there may well be no audit impact. In other cases, the implementation of EDM may be part of a major reengineering of workflow and business processes. The auditor will need to understand the increased

---

[1] In Canada, *CICA Handbook* Section 5360, "Using the Work of a Specialist"; in the US, SAS No. 73, "Using the Work of a Specialist."

[2] In Canada, knowledge of business is discussed in *CICA Handbook* Section 5140 "Knowledge of the entity's business"; in the US, SAS No. 22, "Planning and Supervision," paragraphs 6 to 8.

complexities that the introduction of an EDM system might create in combining office automation with transaction processing.

When an auditor is engaged to audit financial statements of a client who has introduced EDM, several issues have a bearing on the consideration of internal control and the nature, timing and extent of testing required. One important conclusion is that the traditional paper trail diminishes or may vanish. This is discussed in more detail in Chapters 5 and 6. 9

As mentioned in Chapter 3, paragraph 34, one of the important preliminary matters is for the client to have a proper EDM program in place to ensure that evidentiary requirements are met and that adequate controls are in place. The auditor should read the client's program to obtain the appropriate background and business implications of introducing the system and to identify the audit impact of EDM introduction. 10

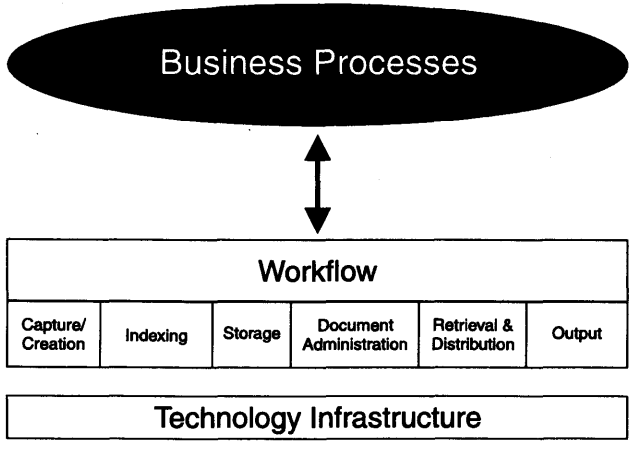
Gathering Preliminary Information

Such preliminary information may include: 11

- *Documentation* — Documentation explaining the general purpose and benefits of the system orients the auditor to the type of EDM system used (for example, workflow management and archive procedures) and provides information about the vendor company.
- *Inquiries* — Inquiries of personnel help determine the system's present and future significance to the company's operations. Available usage reports should be examined to obtain information on the number and types of documents processed per month, the amount of computer resources required and actually used, and costs for the original system, its interim upgrades and maintenance.
- *Standards used* — Preliminary information gathered by the auditor concerning the type of EDM system deployed, its configuration (for example, local versus remote, centralized versus distributed) and the types of documents being processed. The auditor's interest in standards is restricted to how non-compliance with such could result in material misstatements in the financial statements. Available standards include Computer Aided Logistics Support Standards for Department of Defense imaging and other applications, International Standards Organization TC 171 standards for imaging, Canadian General Standards Board, and numerous American National Standards Institute and National Information Standards Organization imaging standards.

Exhibit 1

EDM Components



12 The auditor may wish to accumulate specific information about the EDM process (as set out in Exhibit 1):

- *Capture/creation* — to ascertain how data are entered into the EDM system — scanning, fax, e-mail, or other electronic input (word processing, spreadsheets etc.). To assess control risk in respect of input and access, it may be important to understand the devices/processes used to capture/create input to the system.
- *Indexing* — to know how the information is indexed (manually, OCR, ICR) and what key information is available to perform searches to locate and retrieve documents.
- *Storage* — to be able to access the media to obtain satisfaction over the integrity, security and availability of the documents and to perform appropriate audit tests.
- *Document administration procedures* — for the auditor to have evidence that appropriate general controls (version control, contingency planning, data recovery) are in place.
- *Retrieval and distribution* — to facilitate the audit — the auditor may want to be familiar with any available retrieval and distribution facilities.
- *Output* — to understand if/how the data output from the EDM system are entered into the financial transaction system. It may be important for the auditor to obtain evidentiary support as to the computer controls surrounding the transfer to ensure, for example, completeness and accuracy of data.

Audit Benefits

13 EDM is one of the enabling technologies that change the ways entities do business and, consequently, the way auditors may need to audit in these environments. A well-controlled EDM environment should offer significant

opportunities that may not be available in a paper-document-handling environment:

- It could facilitate the audit planning process by providing a documented model of business process and document flow.
- It may provide for the tracking of documents electronically as they are processed and handled by various individuals.
- The integration of documents into the system can provide a better audit trail than a paper-based system. With the documents that represent the original source documents integrated into the system, it is relatively easy to automatically track information such as when the document was initially created, who modified it later and what decisions were made.
- There may be improved completeness for transaction data because of the automated controls that should be in place.
- There should be improved accuracy for transaction data because of the absence of rekeying.
- It allows the auditor to access both data and the electronic document, thereby possibly reducing the time to audit the transaction and helping to detect problems more readily.
- There may be better internal control because of the consistency of computer processing and, especially in smaller entities, the formalization of processing procedures and controls.
- It can provide the auditor with effective means of designing tests of controls. This may be by comparison of workflow models to actual process and document flows, or by consideration and testing of advanced workflow systems that enforce process and document flow.
- It can help determine the impact of recommendations on document flow by using the modelling techniques provided by the system.
- It can facilitate the use of electronic working papers, where applicable.

Audit Risk

The three components of audit risk (AR) are: 14

- *inherent risk (IR)* — the susceptibility of an account balance or class of transactions to misstatements that could be material, when aggregated with misstatements in other balances or classes, regardless of the existence of relevant controls;
- *control risk (CR)* — the risk that misstatements that could occur in an account balance or class of transactions and that could be material, when aggregated with misstatements in other balances or classes, will not be prevented or detected on a timely basis by relevant controls;
- *detection risk (DR)* — the risk that the audit procedures will not detect misstatements that exist in an account balance or class of transactions and that could be material, when aggregated with misstatements in other balances or classes.

EDM can affect each of these components of audit risk.

Impact on inherent risk

15 EDM may affect financial statement assertions because it may have an impact on the form in which transactions are entered into an entity's accounting systems, including the initiation of transactions. As a result, it is important that adequate preventive controls be in place to safeguard the system and to ensure its accuracy.

16 In addition, since paper evidence is eliminated and electronic media may be inherently more susceptible to undetected manipulation, inherent risk is often higher in a direct-impact EDM system.

Impact on control risk

17 An increased dependence on the computer operations, which is one effect of EDM, will have internal control implications. To maximize the potential business benefits of an EDM operation, it is important to have sufficient controls to ensure document authenticity. Without sufficient controls, there is a potential for undetected errors that can create business risks and losses. These controls provide the opportunity to perform tests of controls as a basis for assessing control risk below maximum. Chapter 5 discusses the controls that should be in place in an integrated EDM operation.

Impact on detection risk

18 Detection risk is the last variable in the audit risk equation (AR=IRxCRxDR). Since the auditor normally wants to keep the level of overall audit risk at a constant level, the impact of EDM on detection risk will vary according to the assessed impact on the inherent and control risk. As mentioned earlier, inherent risk should increase. Control risk may increase or decrease depending on whether the auditor is able to perform appropriate tests of controls. If both risks are higher, or the increase in inherent risk is not offset by a decrease in control risk (that is, there are compensating controls), additional substantive testing will be necessary to reduce detection risk so as to maintain the same overall level of audit risk. Alternatively, the increase in inherent risk could be mitigated if the auditor is able to assess control risk at below maximum and thus allow the auditor to accept this higher level of detection risk without increasing overall audit risk.

AUDIT APPROACH

Preliminary Assessment

19 The auditor is required to obtain an understanding of internal control sufficient to plan the audit, irrespective of the audit strategy used for specific financial statement assertions. After obtaining that understanding, the auditor makes preliminary control risk assessments for relevant financial statement assertions relating to significant account balances or classes of transactions. This preliminary assessment may be at maximum or at a lower level.

20 The auditor could potentially use an audit approach emphasizing tests of controls or one emphasizing substantive procedures or one that uses both types

of tests in varying degrees, depending on the circumstances. This would occur when benefits that result from reducing the extent of substantive procedures or modifying their nature or timing exceed the costs of obtaining and documenting more knowledge about internal control and performing appropriate tests of controls. For example, the auditor may choose to assess control risk at maximum because it is more efficient to obtain the necessary audit evidence by performing substantive procedures than by performing tests of controls necessary to support a lower assessed level of control risk.

Tests of Controls Approach

To use an approach that emphasizes tests of controls, the auditor needs to be able to assess control risk below maximum. Assessing control risk is the evaluation of the design and operating effectiveness of control activities in preventing or detecting material misstatements in financial statement assertions. 21

To support an assessment of control risk below maximum for a relevant financial statement assertion, the auditor should: 22

- have identified specific controls that are likely to prevent or detect material misstatements in that assertion;
- plan to perform tests of controls to determine whether such controls are operating effectively.

The auditor may need to look at general computer controls as part of the determination of the most cost-effective strategy. It should be noted that effective general and application controls will be important for effective EDM transaction processing. As a result, there should be a number of effective controls, and the auditor may be able to assess control risk below maximum, if that approach is considered to be the more effective. 23

Tests of controls can be used to assess the design and operating effectiveness of controls. These need to be performed to assess control risk below maximum and, ultimately, to determine the level of substantive testing that might be needed. These tests include verifying logs, written procedures, documentation, tracking systems and ongoing support/development environment. This involves knowledge of the controls that should be present (addressed in general in Chapter 5 and Appendix A) and knowledge of the audit techniques that might be followed. 24

Alternatively, there may be situations where an approach emphasizing substantive procedures, or one using both tests of controls and substantive tests, may be preferred. The use of substantive procedures will often require a knowledge of appropriate computer-based audit techniques. This approach is discussed in more detail in Chapter 6. 25

Appendix A also sets out a general audit program that might be considered when auditing in an EDM environment. 26

Chapter 5

CONTROLS AND AUDIT IMPLICATIONS

This chapter discusses general computer controls and application controls as they apply to EDM. It also addresses their audit impact.

INTRODUCTION

Control objectives for EDM systems are essentially the same as those for any system. The nature of some risks and the potential impact of a control failure, however, may differ. This will affect the types of controls that an auditor may find. An additional impact of EDM is the potential absence of paper documents and, thus, the transformation of an important traditional body of audit and legal evidence into a different medium. 1

Key Issues

As mentioned earlier in this study, document authenticity is very important from both a business and an audit perspective. To be satisfied that the electronic document accurately replaces the paper original is important due to its interaction (or support for) the electronic financial system of the client. This may require that a number of input controls be present to ensure that accurate capture, version control and access control to the system is achieved. It also requires that adequate controls exist to ensure accuracy of output to the financial transaction system. These and the other controls that are important in an EDM system are the focus of this chapter. 2

As mentioned in Chapter 3, a proper EDM program is important to ensuring that evidentiary requirements are being met. These guidelines are a logical extension of standard procedures for records management and computer processing. An entity that goes about its program in a logical, controlled, authorized and documented manner is likely to conform to the standard. The auditor should obtain evidence that the client has adequate controls to ensure that: 3

- Proper documentation exists — Procedures and systems involved in the capture, storage, retrieval and processing of EDM transactions should be adequately documented.

- The EDM plan is endorsed, in writing, by the top executives within the entity.

CONTROLS

General Computer Controls

Introduction

4 General controls are controls over the activities and resources of the information systems development, processing and support functions. They include segregation of incompatible functions and information systems security activities. General controls are those relating to the environment and operations, as well as physical security and system design. Implementing adequate back-up and recovery schemes for the index and document files is essential. These should not differ from standard electronic data processing controls simply because document files require high-density media to store large files. Back-up media may include magnetic tape, optical disk and others, such as digital audio tape (DAT).

Segregation of incompatible functions

5 Part of the logical security control for EDM is preventing users from accessing unauthorized functions. This is important, for example, when multiple EDM applications reside on a single hardware system. For example, a system that processes accounts payable transactions might segregate the three processes of scanning an invoice, retrieving an invoice and approving it, and retrieving the invoice and inputting a payment transaction. This could help prevent the initiation of fraudulent payments and ensure the accuracy of input transactions. If multiple EDM applications are processed on a single system, it may be important to logically secure the ability to access each application. For example, if documents in support of pending litigation are stored on a system that also contains pending trademark and patent documents, it may be important to logically secure and restrict each group of users to its own applications. This can be accomplished through the use of specific application controls and/or system controls that manage and authorize access to data and application transactions.

Access controls

6 Controls ensuring only authorized users have access to document management systems are essential in an EDM system. For example, images of confidential contracts that may have been stored in locked vaults and are now stored in electronic form will have to be secured by measures that ensure the contracts are not read or altered by unauthorized individuals. The entity should determine the confidentiality and level of data integrity required for documents stored in electronic form and develop and enforce appropriate access controls to ensure that only authorized users have access to the index and document files.

7 Maintaining appropriate access controls surrounding documents, indexes, annotations, and text files can prevent unauthorized individuals from, for example:

- manipulating the bytes of an electronic document file (for example, the corresponding pixels making up the document can be altered);
- changing the underlying index to point to another document;
- tampering with an index file, endangering the system's ability to locate and retrieve files;
- changing or deleting annotations to a document;
- changing or deleting the contents of a text file.

In addition to access controls, system security controls also address the physical security of the data, including backup and recovery procedures. 8

As with other data processing systems, it is not necessary to give every user access to every EDM or every EDM-processing function. EDM-processing system functionality can range from the user being given access to the index only, to the user being able to display, print or fax the document. System security administrators are responsible for establishing user privileges based on need. The extent to which EDM systems are open for viewing will vary according to data classification and the class of user. Access to the index and EDM files should be determined by the requirements of the enterprise. 9

Physical security for the hardware for an EDM system should equal that implemented in a traditional electronic data processing environment. There are, however, some subtle differences. For example, while optical media are much more durable than traditional magnetic storage technology, they are not impervious to disaster and can deteriorate over time. It is important to recognize this when designing back-up and disaster recovery procedures. Also, while EDM files are usually stored optically, the index can either be stored optically or stored on vulnerable magnetic disk devices that should be secured. 10

Another security issue unique to the EDM environment involves access to retrieval workstations and scanners. The considerable cost of these devices warrants giving them extra protection. Security measures should incorporate added controls in such situations. 11

The authorization process requires the introduction of physical and logical security. The objective of physical security is to control access over where the documents stay in the system. Physical security includes locking doors to the computer rooms, securing tape and optical volumes, and a wide array of other methods to restrict access to information. 12

An important objective of logical security is to enforce the division of duties as a preventive control. For example, a sales person should not have the authorization to convert the latest sales order and invoice form into the system. A second objective should be to prevent outsiders from breaching or penetrating the conversion process. Insiders, rather than outsiders, cause most violations. If the EDM system is not secure, the control objectives cannot be met. To meet these control objectives, each step of the document conversion process should be carefully defined when planning the conversion process. Not all control 13

objectives are easy or cost effective for EDM. Therefore, the planning phase, by design, is an important step during the conversion process.

Back-up and recovery and contingency planning

14 These were discussed extensively in Chapter 2, paragraphs 58 to 62.

Program development and change controls

15 To ensure that data are processed accurately, it is important in any computer environment that any development of, or changes to, application programs be properly controlled. With respect to development, it is important that standards be established by the client to ensure the efficiency and effectiveness of the system under development. As well, procedures should be established to ensure that the systems are developed in accordance with the standards. Also, there needs to be adequate management of authorized access to programs to prevent unauthorized modifications to them. All changes to programs need to be adequately controlled.

Application Controls

16 General controls are so named because they are intended to function consistently across all applications. In contrast, application controls are built into specific programs or user procedures and will vary from application to application. They are used to provide assurance that all transactions are authorized, recorded and processed completely, accurately on a timely basis and to provide assurance that the output from the systems is properly controlled.

17 If general controls appear to be strong and have operated effectively throughout the period, the auditor can, by testing the general controls, obtain assurance in connection with each and every application. If, however, weaknesses were found or it was established that there were periods when the general controls were not operating effectively, they would have to be looked at on an application-by-application basis, focusing on the applications that were significant. In this case, a "consolidated" evaluation of general and application controls would be needed to assess the impact of any weaknesses.[1]

18 Two types of control activities contribute to control over application systems:

- Manual control activities carried out by a user of a specific application system. These do not depend on the effectiveness of general computer controls.
- Manual follow-up activities that use computer-generated output or automated programmed control activities (such as edit checks) contained within the computer program. These controls depend upon the effectiveness of the general computer controls.

---

[1] This was adapted from J.E Boritz, *Computer Control & Audit Guide, 9th edition* (Waterloo, Ont: University of Waterloo, 1995), p. 73.

It should be noted that most controls are of the second type.

An example of a manual control of the first type is ensuring the quality of the scanned document. Typically, this involves some sort of visual check of the quality of the electronic document coupled with a review to ensure the correct index entries have been keyed. A quality assurance (QA) scheme supporting the business requirements of the enterprise should be employed. Some QA schemes require that the document be verified against the original document, while others require an operator to verify that the index entry matches the electronic document. 19

An example of the second type of manual control activities is the verification of operations logs (for example, capture and back-up/recovery) and review of activity (audit trail) logs. 20

Control stages

Controls for EDM need to exist at three stages: 21

- capture/creation stage;
- indexing stage; and
- storage stage.

The control discussion that follows uses these three stages.

EDM Application Control Objectives

	Capture/ Creation	*Index*	*Storage*
Completeness	Par. 23	Par. 25-29	Par. 30
Accuracy	Par. 33	Par. 34	Par. 35
Authorization	Par. 37	Par. 38	Par. 39
Information integrity		Pars. 40 - 45	
Audit Trails		App. B - Par. 8	
Supervisory		App. B - Par. 8	
Disposal & Destruction		App. B - Pars. 9 - 10	

Application control — completeness

To achieve this objective, all converted pages of a document are entered into the system and remain in the system during conversion. Controls for completeness are associated with the process of recording, capture and creation of documents. The completeness objective is not concerned with the actual information contained on the documents or in the index. 22

At the capture/creation stage, all source records authorized for capture/creation on transitional storage should be processed according to the 23

client's EDM program. In the case of scanned images, to ensure that the conversion process is complete, the number of pages and the number of documents that are inputted into the system should be validated. In addition, each document should be indexed. This means that every page of a document should be converted, inputted, indexed and released into the system. Any redundant pages of a document and any redundant documents should be accounted for. Control activities should be established for retaking or correction of redundant documents. The date and location/terminal of capture and subsequent modification or update and capture of documents should also be documented.

24 At the indexing stage, all bibliographic and biographic information required by the EDM program should be captured completely.

25 Controls over the conversion process include the quality of indexing information used to locate the converted document. Because most EDM systems store the indexing information in a database, controls governing accuracy, completeness, and authorization for database data entry are similar to entering indexing information — with one major exception. Controls should exist for both data entry and for matching the index with documents.

26 There are two methods of indexing information in an EDM system. The first method is the manual data entry method, possibly assisted by templates for common document types, and the second method is the automated optical character recognition (OCR) method. Documents are usually manually indexed at a workstation and OCR servers extract index data using the OCR method. In both cases, quality controls should be established to ensure that every document and every folder contains proper index values.

27 Controls for accuracy of indexing information begin by determining the critical data index fields. Once that is done, the degree of control over each index should be determined. For example, while an account number is manually indexed, a critical field can be validated against a master list of account numbers. As another example, if OCR records the check amounts, then the amounts should, as a minimum, be range validated for committing the data into the system. An index value that does not correspond to the converted documents should be reprocessed.

28 Bibliographic information, created by the client for the purpose of locating specific documents, should be consistent and include:

- subject matter of the document;
- description of the document;
- classification number;
- location of the document;
- any information concerning reference/transfers or changes to the index;
- normal/scheduled retention and destruction dates; and
- cross-referencing information about the document record.

To be complete, biographic information for locating and retrieving documents should have the following: 29

- exact date of capture;
- capture device location or identification;
- any details on modifications that took place; and
- cross-referencing information.

At the storage stage, control techniques should ensure that documents captured by an EDM system are not lost or damaged through accident or omission. There should be basic protection against disaster, mischief, accidental erasure and unauthorized annotation or replacement. 30

Application control — accuracy

To achieve this objective, document pages are captured in a manner that preserves critical information during conversion. Controls for accuracy ensure that the capture/creation of the document is correct, for example, that an image is a human-readable representation of the converted page, and the index for the document is correct. Because images contain static data and (de)compression processing is slow, data modifications and updates are often infrequent after a paper document is converted to image with its index. Therefore, the accuracy of the conversion process is perhaps the most crucial control objective to be established and maintained for an EDM system. 31

Error handling procedures need to be established and updated on a continuing basis for document preparation, scanning and filming, quality control indexing and document release. Simple definitions and examples of what constitutes an error condition should be established while planning for EDM conversion. Delays or errors in document preparation could translate into problems during the conversion process. Error handling procedures should include accounting for missing documents and misfiled or incorrect pages. Scanning and filming errors should be quantified and corrected using a set of predefined procedures. For example, document scanning error codes can be used to rescan or refilm a batch of pages scanned too lightly. Similarly, procedures for documents that fail quality control or for misindexed documents need to be established. There should also be procedures to deal with additional inputting/verification of illegible original documents by user departments. Finally, scanned documents that fail to be written to disk files should be marked as errors and reprocessed. This could be done by placing the error documents on an error queue, correcting the error and releasing the documents from the error queue. 32

At the capture/creation stage, documents captured by the document management program to transitional storage need to be captured accurately and reliably. The document recorded on transitional storage needs to comprise the whole of the source record(s) in a way that does not compromise its status as a facsimile. 33

34 At the indexing stage, all bibliographic and biographic information captured needs to be accurate for the purposes for which it is intended (for example, to locate and retrieve specific documents, and to reflect historical data about those documents).

35 At the storage stage, there should be controls to ensure that data created/captured during the process are accurately converted to secure storage. In the event that the initial capture is to transitional storage, the conversion should occur within a reasonable period of time.

Application control — authorization

36 It is important in an EDM system that only authorized documents are processed and maintained in the system.

37 At the capture/creation stage, documents captured by the system should be authorized as set out in the EDM program. In addition, digital signatures (for time and date) could be used to authenticate the document characteristics (for example, time, date and contents).

38 At the indexing stage, controls are needed to ensure that only authorized bibliographic and biographic information are captured in the EDM system. Authorization should be obtained in accordance with the authorized procedures manual, if such exists.

39 At the storage stage, there should be controls to ensure that there is proper authorization to convert documents to secure storage. This would include:

- only documents captured within the authorized EDM system should be converted to secure storage;
- the time for conversion should not be excessive, given the task to be performed;
- the time for conversion should also be commensurate with the need for quality control; and
- disposal of source records should not occur until conversion to secure storage has taken place.

Application control — information integrity

40 Information integrity relates to both the electronic document and its underlying database index, since both are electronic files.

41 Current technology does not allow changes to be made readily to the actual document; document files can, however, be compromised. The following are a few specific instances where document integrity could be impaired:

- the original authoring tool can be used to re-open and directly alter a document;
- when manipulating the bytes of an electronic document file, the corresponding pixels making up the document can be altered;
- although WORM technology precludes writing over an existing document, a document can be replaced by changing the underlying index to point to a copy or another document;

- the annotation of a document might be changed (an annotation is a note file stored separately from the document but retrieved at the same time) or deleted;
- the index file might be tampered with or damaged, which endangers the system's ability to locate and retrieve files; or
- documents are assigned previously allocated numbers, causing retrieval errors.

Risks related to the integrity of both document and data information can be managed. Traditional data integrity controls should be used where appropriate and new controls are being developed to address integrity issues unique to document processing. 42

There should be adequate provisions for the maintenance, preservation and confidentiality of documents in an EDM program. Such provisions could be described in the procedures manual. Control techniques should ensure that documents captured by the EDM program are not subject to unauthorized alterations. 43

There also need to be controls to ensure that the biographic and bibliographic information related to documents captured by the EDM program cannot be lost or damaged through accident or omission. Basic protection for biographic and bibliographic information includes protection against the risks discussed in the next paragraph. 44

Finally, there should be control techniques to ensure that information captured by the EDM program cannot be lost or damaged through accident or omission. Basic protection for documents could include protection against: 45

- disasters;
- mischief;
- accidental erasure; and
- annotation or replacement that is not authorized.

Relationship of Controls with Financial Transaction System

Where the EDM system has a direct impact on a financial transaction system, the traditional financial transaction system controls should exist to ensure that, once the transaction is captured (into the financial transaction system), it is processed accurately and completely. In addition, the controls of the EDM system will be of benefit: 46

- To avoid re-processing and to ensure that only authorized transactions are entered into the financial transaction system. For example, electronic flags can be created for each document once initial authority is provided, and activated once the document's information is transferred to the financial transaction system. Because the flag cannot be reset, duplication of input can be avoided.
- The use of properly controlled OCR will assist in ensuring the accuracy of input into the system.

Application Controls and Relationship to Financial Statement Assertions

Completeness

47 In a more traditional computer application, batch totals and sequentially numbered documents and other control procedures, such as hash totals, would typically be designed to meet this control objective. In an EDM environment, controls, such as those discussed in paragraphs 22 to 30, could be appropriate.

Existence/occurrence

48 Controls for accuracy, authorization and information integrity, as discussed earlier, allow the client to verify that the electronic data received are *bona fide* and have not been altered. They can be used to detect situations where there have been changes, whether accidental or deliberate.

Valuation

49 Pricing information for a transaction may come from an electronic input document. The controls for authorization and data integrity for any processing changes have to be followed.

Measurement/ownership (rights and obligations)

50 A liability does not normally exist until the goods are shipped or received, depending on the agreement and the shipping terms expressed in the purchase order. A transaction log file may indicate that a liability should be recorded when it is updated with information entered from its receiving department. Or the liability might arise when the shipping notice from the supplier is scanned into the system. Again the controls for accuracy and integrity are important.

Presentation

51 Controls to ensure proper classification are similar to other advanced automated systems. Normally, the auditor would expect to find cross-reference tables using an identifier, such as a part number or customer/supplier number, that assigns appropriate classifications for posting and/or reporting purposes. Details on the initial purchase order could also help in determining the proper classification.

Complying with Regulations and Standards

52 Controls are necessary to ensure adherence to government regulations in all the document-processing system policies and procedures. In the consumer loan environment, for example, documents such as the signed agreement and titles should be kept and stored off-site in a secure environment, while correspondence, credit reports and the loan application itself can be destroyed after scanning.

53 Compliance also involves adherence to industry standards. While standards remain somewhat *de facto* in nature, a number of entities — such as the Association for Information and Image Management (AIIM), the Department of Defense CALS, the Canadian General Standards Board — have established guidelines with which document-processing systems may need to comply. In

addition, there is other draft legislation, such as the Proposed Uniform Evidence Act (Canada), that also prescribe guidelines to ensure that documents are admissible.

In addition, there should be conformity to applicable technological standards. 54
The standard used by the client for capturing, storing and retrieving the EDM transactions should be generally accepted as a widely used standard for technical components (for example, compression and scanning).

Chapter 6

AUDIT APPROACH

This chapter discusses considerations in determining an audit approach in an integrated EDM system and provides examples of possible techniques to follow.

INTRODUCTION

After obtaining a sufficient understanding of internal control to plan the audit, the auditor may make preliminary control risk assessments for relevant financial statement assertions relating to significant account balances or classes of transactions. In some circumstances, even though control activities have been identified, the auditor may choose to assess control risk at maximum because it is more efficient to obtain the necessary audit evidence by performing substantive procedures than by performing tests of controls necessary to support a lower assessed level of control risk. 1

As addressed in Chapter 4, the auditor could use: 2

- an audit approach emphasizing tests of controls; or
- an audit approach emphasizing substantive procedures.

In many cases, depending on the circumstances, it is also possible to use an audit approach that uses both tests of controls and substantive tests in varying degrees. This chapter discusses the attributes of each approach and provides examples of tests.

TESTS OF CONTROLS APPROACH

In the opinion of the Study Group, the most effective and efficient audit approach is to first obtain evidence that document authenticity exists, ideally using tests of controls. To use a test of controls approach that reduces the extent of substantive testing that might otherwise be needed, the auditor needs to obtain evidential matter to support an assessment of control risk below maximum by: 3

- identifying specific controls that are likely to prevent or detect material misstatements in that assertion;
- performing tests of controls to determine whether such controls are operating effectively.

4 In respect of document authenticity, the auditor may need to have evidence that:

- all electronic documents are complete;
- there is proper identification of who created them;
- there is proper identification of who modified them; and
- the data contained in the documents are accurate.

5 To obtain this evidence, the auditor may have to obtain satisfaction that:

- the general computer controls appear to be effective and would support an assessment below maximum; and
- the application controls for the EDM system appear to be effective and would support an assessment below maximum.

The relevant controls were addressed in Chapter 5.

6 If the auditor is satisfied, through this testing, that document authenticity exists, the auditor should be able to effectively use the EDM system in performing the audit. Once transactions are selected from the financial transaction system, the auditor can then refer to the electronic documents contained in the EDM system as support for the transactions. This should substantially reduce the time required to obtain the supporting evidence for completeness and accuracy.

7 Where document authenticity does not exist, the auditor may need to ascertain whether the client maintains suitable paper evidence to support the appropriate financial statement transactions. If third-party paper evidence is maintained, the auditor may have to use it when testing. Although this would likely be just as effective as the approach outlined above, it likely would be far less efficient.

8 Appendix A describes a number of controls and procedures for testing the controls of an EDM installation. The material in paragraphs 15 to 32 below describe how computer-assisted audit techniques can be used to help an auditor test controls.

SUBSTANTIVE TESTING

9 In the absence of effective general and application controls (and, thus, the lack of document authenticity) and the absence of paper, the auditor will need to determine whether any other evidence exists. This situation would be similar to one where the client's original documents have been destroyed, but photocopies of information are available. The auditor may find it necessary to do extensive third-party transaction confirmation and test subsequent account balances. Although this may not be efficient, they may be the only procedures that could be undertaken.

10 Some of the tools and sources of evidence that the auditor would need to consider include:

- Use of sampling — To be able to reach an opinion about a significant balance or class of transactions, the auditor may need to use some sampling

method (including statistical) to select items for testing from the financial transaction system. The extent of testing would likely be significant, since control risk would be higher.

- Comparison — To select items for testing and to identify possible problem accounts, it could be useful to use analytical procedures, such as comparison of client data to industry data, similar prior-period data, client-determined expected results, auditor-determined expected results and expected results using non-financial data.
- Confirmation — This would involve confirmation of transactions (for example, purchases with a supplier). Confirmation could be done on a total or selected-item basis, depending on the nature of the test.
- Subsequent transactions — Testing subsequent transactions could be conducted to assess the reasonableness of the account balances.

As mentioned above, although not efficient, these procedures may be the only ones that could be undertaken. If they are not sufficient, the auditor will have to assess the impact of this deficiency on the scope of the audit.

It is anticipated that an approach that uses both tests of controls and substantive testing may likely be the most cost-effective and efficient for an EDM system (the auditor is required by generally accepted auditing standards to use some substantive procedures to obtain sufficient audit evidence, the extent to which will vary according to the assessed levels of inherent and control risk.) The auditor will look at: 11

- materiality;
- inherent risk and control risk situations;
- the experience gained during previous audits as to the reliability of the client's records and representations;
- the persuasiveness of the evidence; and
- error or fraud found while performing audit procedures.

This chapter provides examples of substantive tests that could be undertaken, as well as computer-assisted audit techniques that can be used.

The techniques discussed in these paragraphs deal predominantly with transaction-level testing. As they relate to an EDM system, these techniques include random sampling and activity auditing. 12

Random sampling

The sample would be taken from the financial transaction system. Documents can be randomly retrieved and displayed via a workstation and printer to check for index accuracy and legibility. 13

Activity auditing

An example of activity auditing is the testing of the audit trail/tracking system. Here, a range of activities is performed with a document, including scanning and retrieval. The tracking database and reports are checked to verify that all activities were recorded. Scripts and checklists can help facilitate this process. 14

COMPUTER-ASSISTED AUDIT TECHNIQUES

15 When gathering audit evidence, the auditor should consider the use of computer-assisted audit techniques (CAATs). Depending on whether or not the client keeps hard copy input, the auditor may have to be familiar with computer-based audit techniques to obtain audit evidence of an EDM transaction. The purpose of this section is to discuss some of the testing methods currently being used to audit an integrated EDM system and some that are more advanced. Currently used techniques involve the use of client query facilities and data extraction and analysis (audit) software. Advanced techniques include the use of integrated test facilities, imbedded audit modules and concurrent audit tools. This section also addresses the possibilities and limitations of some methods of testing. It does not, however, address all of the procedures that could be used in testing a traditional computer system.

Remote Access

16 If the client provides the auditor with the ability to access its systems from remote locations, the auditor may be able to select samples and do appropriate testing without being on site and disrupting the work of the users/employees. This would be the case if the auditor uses client query facilities or data extraction and analysis software. The client should provide the auditor with appropriate passwords, and the auditor should ensure that client access controls are not compromised.

Use of Client Query Facilities

17 One of the easiest and most common computer assisted audit techniques is the use of client-installed query functions and report writers. This software is normally easy to use and quite powerful. One disadvantage is that the software is usually unique to its particular environment. As a result, the auditor normally has to become familiar with the software each client uses. Another disadvantage is that this software usually does not have a statistically-based random selection utility that an auditor could effectively use.

18 To obtain the necessary audit evidence in an EDM environment, the query facilities can be used in both the financial transaction and the EDM system.

Data Extraction and Analysis (Audit) Software

19 Traditional audit software can be used in various ways:

- basic integrity checking — for example, do all documents have an index and vice-versa?
- approvals checking — for example, do all documents of type x have approved status if they are over 30 days old? and
- sampling — for example, using various sampling methods, a sample could be selected from the financial transaction system and the software could then be used to retrieve all index data and document data for the appropriate documents chosen (thus providing evidence for the sample selections).

There are various disadvantages to using data extraction and analysis software. Usually, the most significant problem is obtaining the data in a format that can be used effectively. 20

Advanced Techniques

Embedded audit modules

Embedded audit modules are programs written and compiled within an application to perform audit procedures concurrently with the operation of the application. These modules may run routinely or function only when specifically activated. 21

Embedded audit modules enable continuous monitoring and analyzing of transaction processing. They are particularly effective in high-volume, on-line, real-time systems, in which timeliness, completeness, accuracy and validity of transactions are essential. Such systems do not lend themselves to manual auditing. In many situations, embedded audit modules are implemented for the applications that pose the highest risk for the entity. 22

The use of embedded audit modules offers several audit advantages: 23

- the auditor can continuously monitor systems;
- the auditor can select specific data samples at any time because the data are selected simultaneously with the normal production process;
- they encourage auditor involvement during the system design phase.

The primary reason for the use of embedded audit modules in an EDM environment is the loss of a visible audit trail. In many cases, the embedded audit module can be extended with exception reporting and file interrogation facilities. This will give the auditor an effective way to detect unauthorized data modifications. 24

These modules are complex, advanced audit tools. The auditor can use them to select items for testing or evaluation (for example, deviations from predetermined purchase and sales policies, and the frequency of certain types of transactions). 25

Embedded audit modules are useful in monitoring the performance of the application system on a continuous or selective basis. Even though most systems are designed to prevent and detect errors, errors can occur because of defects in the system's development or because of incorrect or improper modifications to the system. Embedded audit modules provide the auditor with an independent check on the performance of the application system and provide an opportunity for timely corrective action. 26

Currently, embedded audit modules are not widely used because: 27

- The time, effort and resources required to build and maintain them can be substantial.
- They must be protected against unauthorized modifications.
- They normally must be built during the development of a new system; failure to do so will significantly increase their costs at a later date.

- Typically, because of the interrelationships between the module and the application, modification of the application requires modifying the audit module.
- They require a high level of data processing/programming skills.

28 The reengineering of business processes and systems that occurs during the EDM implementation may provide the auditor with the opportunity to include embedded audit modules in the reengineered systems. Consequently, their use could increase in the future.

Concurrent audit tool

29 In general, a concurrent audit tool is similar to an embedded audit module in that it inspects the transaction as it takes place. The main difference is that it is designed and controlled by the auditor and linked into the entity's information system rather than being part of the system.

30 A concurrent audit tool allows an auditor to evaluate the client's controls at the time a transaction is processed, without disrupting the client's normal operations. The concurrent audit tool could be linked into the system for a period of time to perform tests and provide audit evidence.

31 In a situation where a client has ineffective controls, a concurrent audit tool gives the auditor the opportunity to perform analytical procedures and substantive testing, because the data have been captured by the tool. When client controls are strong, the auditor can also use the tool for the testing of controls.

32 One of the advantages of this tool is the fact that it is designed and controlled by the auditor. As a result, the potential for unauthorized modification is reduced. The disadvantages are similar to those for set out for embedded audit modules.

Appendix A

SAMPLE CONTROLS AND SAMPLE AUDIT PROGRAMS

GENERAL ISSUES

Controls and audit programs in an EDM environment are similar to ordinary computer application files. As discussed in Chapter 1, they are applied to a different set of data. In addition to performing appropriate document sampling and gathering preliminary information, the auditor may wish to gain an understanding of physical security, system security and other controls. 1

CONTROL AREAS

The EDM process should be carefully controlled. Certain control areas can serve as checkpoints for process assessment. The auditor may wish to test the design and operating effectiveness of controls in areas of possible risk. The following controls for EDM systems could be covered in the audit: 2

- general computer controls — segregation of incompatible functions, security, retention, back-up and contingency planning;
- controls over capture/creation;
- indexing controls;
- document administration controls;
- retrieval and distribution controls; and
- output controls.

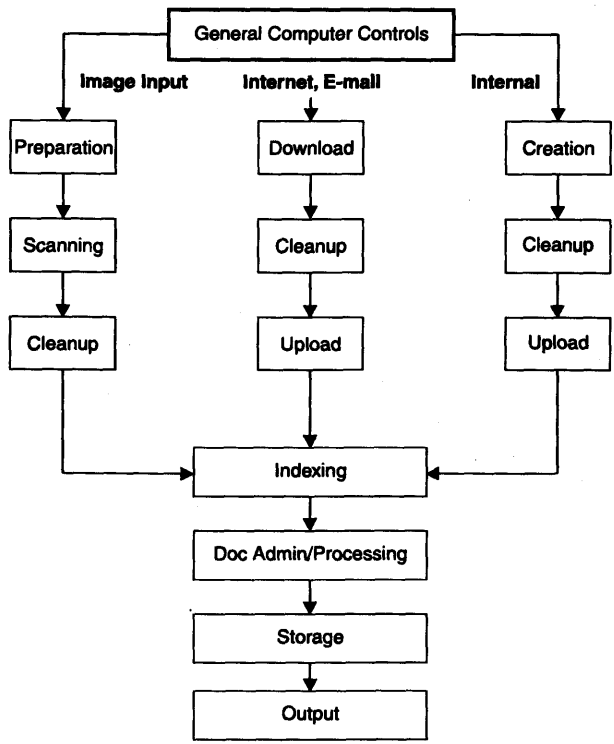
For the purposes of the discussion in this appendix, the input controls over capture/creation will be segregated according to the significant types of input to the EDM system: 3

- imaging;
- other external sources, such as e-mail, Internet, fax;
- internally created electronic documents.

An overview of the appropriate controls is set out as Exhibit 1.

Exhibit 1

EDM General Controls



GENERAL COMPUTER CONTROLS

Security

4 A wide range of controls, including both physical and logical controls, should be present to ensure thorough protection of the EDM system. These include the areas discussed below.

Physical security

5 The auditor should gain an understanding of an EDM system's environment. For example, an optical jukebox should not be exposed to excessive moisture or temperature levels. Individual optical disks can be cleaned with virtually no effects on the integrity of data. In addition, magnetic fields have no effect on the readability of disks after they have been removed from the jukebox. Magnetism may, however, adversely affect the writing of data on to optical media while inside the jukebox, because of its effect on the laser.

System and application security

Security controls should be implemented to prevent unauthorized access to both the document and the index file containing descriptive information about the document. An individual must first gain access to the index to determine which document is to be accessed. Therefore, index files should be just as secure as the respective document files. 6

Compression modules provide a method for efficient and secure storage because data are stored in an encrypted form. Because decompression software can be used to read restricted information if other preventative security features are not implemented, access to compression and decompression software should be adequately controlled to detect and report occurrences of its use outside of normal operations. Adequate operating-system level security, augmented with application security controls, can help ensure that only authorized personnel access documents. 7

IMAGING CONTROLS

Most application systems allow edits to be performed after storage has occurred. With optical media, however, data cannot be changed after being stored. Input controls for imaging present checks and balances to prevent incorrect or incomplete data storage. 8

Document Preparation

To begin with, the auditor should gain an understanding of the controls within the document preparation function. If documents have not been prepared in a controlled manner, information may be stored without review or approval for quality, accuracy, currency or completeness. Documents should be prepared by staff who understand the information contained in the documents. Staff should also be qualified to handle sensitive documents and operate all hardware and software required for information input. Generally, the individual performing document preparation also inputs documents for scanning and creates file indexes. As a contingency, a second person should be trained on input operations in the event the primary resource person is not available. 9

The document preparation function should: 10

- prevent duplicate documents from being entered;
- investigate the location of missing documents;
- move incorrectly associated subordinate documents to their correct master documents;
- eliminate unnecessary information from documents;
- ensure documents reside in the correct input batch;
- maintain accurate records of documents scanned to date.

Scanning

The user department's management should establish the priority of documents to be scanned. Scanning and input software require control of device and software configuration settings. These include: 11

- appropriate values for image quality (the dots per inch value) to enable the user to read information with the appropriate degree of definition;
- threshold values being set to ensure that the greatest amount of information from the original document is identified correctly;
- resolution values to guarantee that objects, lines and characters located in close proximity on the original do not appear connected to one another after being entered.

12 In addition, controls over the physical devices used for input should be established to reduce or eliminate mechanical problems during operation. These problems include wrinkling, misfeeding or misalignment of documents. Maintenance agreements should provide for periodic cleaning because dust and other particles in the device can cause speckling and fine lines to appear on resulting images.

13 Staging and storage areas for documents used during input should be environmentally regulated to ensure adequate ventilation and humidity and to reduce the risk of fire and water damage.

Cleanup

14 Only personnel familiar with the document information should perform the cleanup process, because image cleanup often involves adding and deleting discrete pieces of information to the image file before it is stored in the image vault. For example, if parts of several long lines on an engineering drawing have not been detected by the scanner during input and do not appear on the resulting image, the individual responsible for image cleanup would, among other cleanup tasks, redraw the lines electronically on to the resulting image file to match their location on the original document.

15 Image cleanup is performed to eliminate machine-generated data errors on the image file. The auditor should note that information stored or processed by a system, regardless of whether image cleanup is used, is not identical to the original document. The condition of the original may have changed as a result of document aging or other damage, and exactness may not be necessary. The quality of lines, characters, colours, objects and background will always differ to some degree when the original and imaging system documents are compared. The auditor's objective when comparing documents should be to verify that no image data can be misinterpreted by users because of poor quality, omission of data or inclusion of incorrect data, and that only those authorized to clean up documents can do so.

16 The user department should control changes to information (where practical) through a quality check by reviewing images after image cleanup. This should be done before the changes are stored to optical media.

E-MAIL, INTERNET ETC.

Downloading

Adequate controls to protect the entity from unauthorized access to network resources and applications are essential. Where information/commerce data are obtained through Internet e-mail or WWW sites, there are a number of control considerations: 17

- the entity should not rely on the secrecy or authenticity of information traversing the Internet in public codes;
- a single point of connection to the Internet should be used;
- connection to the Internet should be made only with equipment dedicated to that purpose (servers and firewalls);
- protection should be layered;
- end-to-end encryption should be considered for commercial applications to keep data private;
- all events and traffic should be monitored and logged.

For e-mail, it is important to have appropriate security to ensure confidentiality and integrity of message contents. Some of the emerging security practices include: 18

- using appropriate dial-in access software control;
- using limited function e-mail gateways;
- using firewalls;
- using bulk point-to-point encryption on key network paths;
- using public key encryption keys to ensure that information can be read only by intended recipients.

Cleanup

Consistent with the above discussion on imaging, it is important that the data received in this manner be "clean" and in a format that can be used in the EDM system. Cleanup is performed to eliminate any transmission-related errors that might have occurred or to remove malicious/harmful code or masquerading by unauthorized users. Again, only personnel familiar with the document information should perform the cleanup process. The auditor's objective when comparing documents should be to verify that no data can be misinterpreted by users because of poor quality, omission of data, or inclusion of incorrect data, and that only those authorized to clean up documents can do so. 19

The user department should control changes to information (where practical) through a quality check after cleanup. This should be done before the changes are stored to optical media. 20

Uploading to EDM System

Controls need to exist to ensure that the transfer of data to the EDM system is properly controlled. Logical access controls are needed to prevent unauthorized access to the network and to ensure that only *bona fide* transactions are transferred. 21

INTERNAL DOCUMENT AUTHORING

Creation/Authoring Tools

22 Controls need to exist to ensure that unauthorized users do not have access to the tools and programs to create documents for input into the system, and that the EDM system will not accept a document from an unauthorized user. At the creation stage, controls should exist to ensure that the document is created in a proper format and that the document is accurate. This may necessitate a subsequent review by the author or by another reviewer before the document is transferred to the EDM system.

Uploading to EDM System

23 In most instances, the system is integrated and uploading of data is instantaneous. Again, controls need to exist to ensure that the transfer of data to the EDM system is properly controlled. In this case, proper LAN controls are necessary to prevent unauthorized access to the network and to ensure that only *bona fide* transactions (such as the correct type of transaction given the system) are accepted by the EDM system.

INDEX CONTROLS

24 Each document's retention period, destruction date or scanning date should be accessible from the index, indicating the appropriate time period that the document should remain on the system. There should be a standard date recorded in a standard database format. This date can be generated by the application automatically or inserted by the system software. Without the date, the user will have no baseline from which to determine which documents are obsolete. In general, the index should contain enough information to ensure the document's timeliness and accuracy.

DOCUMENT ADMINISTRATION AND PROCESSING CONTROLS

25 Weaknesses in EDM systems can be avoided through attention to solid preventive and detective controls within workflow management.

Workflow management controls

26 Controls should ensure that only authorized individuals change workflows and act on documents at each location in the workflow. Appropriate logs should be maintained to detect changes and other actions.

27 User departments should review and approve workflows after each change and changes should be submitted for efficient routing to the information systems department or the interdepartmental group assigned to improving workflow processes. In addition, periodic checks on the location and status of documents in various locations throughout the entity will validate the integrity of status reports.

28 Timeliness, accuracy, and completeness of reports are important to management's success in correcting inefficiencies. The auditors should determine that documents are routed according to the script and that all

alterations to data are approved. In addition, management staff should review regular reports identifying the status of each document. Attempts should be made to identify recurring bottlenecks in the workflow process to improve efficiency.

Storage Controls

Electronic or manual controls should be present to record changes in EDM file inventory or changes to the order of documents within an electronic file folder. When a file's retention period expires and the document is removed, a corresponding entry should be made in the index indicating the document's expiration, the date that it was removed and the archive information indicating where it may be found in a physical archive or a statement of the document's disposition. 29

Retention periods should be established for the documents being stored. The retention period should allow enough time for errors to be detected and corrected on the document before any original paper document is destroyed. Often, to allow adequate time for error detection, retention periods must be increased when EDM operations begin. 30

Output Controls

Controls over EDM output are similar to those for other application systems and those of original paper documents. Detective controls should be in place to detect who has viewed or printed a document. Authorizations should be maintained to verify any individual's access privileges. 31

Output devices should not diminish the quality or readability of data. The devices should be reviewed by user departments to ensure printed or viewed data quality is maintained at an acceptable level. The level may be gauged by the numbers of errors occurring from misinterpretation. 32

SAMPLING CONSIDERATIONS FOR IMAGING APPLICATIONS

Audits of the imaging systems component may require a greater number of samples to be taken to cover all areas of exposure. Samples may be taken randomly or subjectively (if the auditor has reason to believe breaches of control exist in a particular area). Exhibit 2 aids the auditor in selecting samples to assess control risk in desired areas. It is not intended as an all-inclusive list of items the auditor may need to obtain information about controls during the audit. Rather, it is a tool the auditor can use when determining which documents and images to sample, depending on the levels of control to be verified. 33

Exhibit 3 provides a sample audit checklist for the imaging portion of EDM. The checklist can be used, modified where appropriate, for the other EDM technologies. 34

Exhibit 2

Audit Sample Considerations

The following are sample files the auditor may select during the audit:

Sample Identification Description

A Original master and subordinate documents, taken before document preparation.
B Original master and subordinate documents, taken after document preparation and before scanning.
C Images viewed from a scanning-station monitor, or equivalent.
D Images viewed or printed on paper at a user's output station.
E A complete listing of all index data for selected image files.
F Workflow scripts.
G Workflow status reports or logs, listing the location and status of each image.
H Images viewed at several locations throughout the workflow process.
I Workflow efficiency reports from the user department's management.
J Printout of all stored images in the pattern recognition system.
K System-recognized images viewed from the input station.
L Exception images, viewed from the input station.
M Image-file listing of all files stored to date.
N Log of all image files printed by the imaging system.

The following are several control areas the auditor should consider and, if appropriate, test, and the corresponding samples from Exhibit 1 required for verification:

Input Controls:

- Accuracy and completeness of the document preparation function (Samples A and B).
- Adequacy of scanning and input subsystems and settings (Samples B and C, or B and D).

Editing Controls:

- Adequacy of the image cleanup process (Samples B and C, or B and D).

Index Controls:

- Completeness of index information (Samples A and E).

Processing Controls:

- Verification of image file location and status (Samples D, F, G, and H).
- Timeliness of application reports (Sample I).
- Accuracy and completeness of application response (Samples G, H, and I).
- Completeness of stored images (Sample J).
- Accuracy of the pattern recognition process (Samples B, K, and L).

Output Controls:

- Adequacy of output security (Samples D and N).
- Adequacy of storage, archive and retention management (Samples E and M).

Exhibit 3

Sample Audit Checklist for EDM System Components

This checklist may assist the auditor in gaining an understanding and testing controls of EDM systems.

Document Preparation Controls	yes/no
1. Is document preparation being performed?	_____
2. Have personnel been adequately trained on critical information requirements of the system?	_____
3. Does a sample of documents taken after document preparation, but before scanning, reveal any of the following:	
• Duplicate documents?	_____
• Missing documents?	_____
• Incorrect associations between master and subordinate documents?	_____
• Inclusion of superfluous information on documents?	_____
• Inclusion of incorrect documents in the batch to be scanned?	_____
4. Of the entire document population, are the documents being prepared providing the most timely information to the entity?	_____
5. Is the preparation process being ordered according to priority?	_____
6. Is there a method used by the client to ensure that all documents scheduled for preparation (for example, checkoff lists, batch tickets, signatures) have gone through the preparation process?	_____
If yes, explain:_____	
7. Have documents scheduled for processing been authorized?	_____

Document Scanning Controls	yes/no
1. From an on-line examination of sampled images, do the document quality settings (for example, 200 dots per inch, 300 dots per inch) allow the user to read all information accurately?	_____
2. Is there a maintenance contract or service agreement on the scanner?	_____
3. Does the maintenance contract include periodic cleaning?	_____
4. Is the setting for the scanning threshold appropriate?	_____
5. During an observation of the scanning process or interviews with clients, are there any mechanical problems with document feeding, alignment, or document wrinkling?	_____

6. Is the resolution power of the scanner such that it can detect critical images located in very close proximity to one another? _____
7. Where are documents stored before the scanning process? _____
8. Where are documents stored after the scanning process? _____
9. If the documents are stored in a different location after the scanning process, is it adequate? _____
10. Does documentation exist for the retention periods of scanned documents? _____
11. Are retention periods different than those for documents of the same type which will not be scanned? _____

    If yes, explain:_____

12. Does the retention period allow for errors to be detected and corrected on the image before the original paper document is destroyed? _____

Image Cleanup Controls yes/no

1. Is the image cleanup process being performed? _____
2. Are the personnel performing the cleanup familiar with the documents' information? _____
3. Compare a sample of paper documents to their corresponding digital images for the existence of periods, commas, lines, speckling, and other markings on one image only. Are differences apparent? _____
4. Will the markings, or lack thereof, result in a misinterpretation of information? _____
5. Through a comparison of documents, does the existence of marks indicate that the document did not go through the cleanup process?_____
6. Has information been added to the document? _____
7. Is the new information complete, accurate, and approved by appropriate personnel? _____

Index Controls yes/no

1. Are indexes for image files stored on:
   [ ] Optical media? [ ] Magnetic media? [ ] Magneto-optical media?_____
2. If indexes are stored on magnetic or magneto-optical media, have only appropriate personnel been given security privileges to update the index? _____

3. Is the retention period, destruction date, scanning date, or other information readily accessible from the index that indicates the appropriate time period that the image must remain in the system? _____

4. Is enough information contained in the index to make the accessibility of the image timely and accurate for the users? _____

Processing Controls yes/no

1. Who can gain access to workflow scripts? _____
2. Are all individuals on this list authorized? _____
3. What logs, processes, or reports exist to detect and report changes in scripts? _____
4. If these changes are authorized, how are the changes reported to the users to prepare them for a change in operations? _____
5. Is each script reviewed and approved by a representative of each department/entity involved with the workflow? _____
6. Are images routed to the correct locations? _____
7. Are they routed within the correct time frame? _____
8. At all locations, are appropriate approvals gained before images are routed to the next location? _____
9. Are all document images in one logical folder routed together (master image and all subordinate images)? _____
10. Does an application log exist which tracks activities and locations of each document image? _____
11. At what points (if any) in its life-cycle can the image be altered? _____
12. Can the system detect all occurrences of changes? _____
13. Are management staff receiving reports on the efficiency of the workflow process? _____
14. Does evidence reveal that they review them? _____
15. Do they receive timely reports to make decisions improving the efficiency of the workflow? _____
16. Do these reports contain collective and complete information to result in knowledgeable decisions? _____
17. How are exceptions to the script handled? _____
18. Do numerous exceptions justify a script to be created especially for them? _____

19. Who can change the system templates? _____

20. What processes or logs are maintained to detect or report access or changes to the templates? _____

21. What are the current number of exceptions recorded on average per batch (please list maximums and minimums)? _____

22. How many images are incorrectly identified as legitimate patterns? _____

23. From test documentation, what are the number of exceptions recorded at each interval of changed system settings? _____

24. Are all possible patterns stored in the system? _____

25. Are patterns stored which should not be? _____

26. Are any automated exception-handling methods in place to assist in the correction of exceptions? _____

    If yes, to what extent is the automation used? _____

Output Controls yes/no

1. Who has access to view production images? _____

2. Are these employees different from those who can view paper documents? _____

   If yes, explain: _____

3. Are restrictions placed on when documents can be viewed (such as, after normal business hours)? _____

4. Are controls in place to detect who has viewed, printed and changed an image file? _____

5. Are controls in place to ensure that printed documents are retained until the corresponding images are verified? _____

6. Do output devices reduce the quality of the original image? _____

7. What authorizations are required for access to view or print an image? _____

Storage Controls yes/no

1. Is compression performed? _____

2. Is the compression ratio appropriate, given the compression technique, for the amount of information to be stored on each document? _____

3. Are image files stored on:
   [ ] Optical media? [ ]Magnetic media? [ ] Magneto-optical media? _____

4. If they are stored on magnetic or magneto-optical media, have only appropriate personnel been given security privileges to update the data? _____

5. Are all changes to image files approved? _____

6. Are archive disks being stored offsite? _____

7. Are disks appropriately labelled and logged? _____

8. Are the on-site and off-site storage facilities secure? _____

9. Who has access to the archive? _____

10. Are there appropriate controls for destruction of documents?
    - proper authorizations _____
    - proper scheduling for routine destruction _____
    - special procedures when litigation is present or pending _____

Appendix B

SOME LEGAL CONSIDERATIONS FOR DOCUMENTS ORIGINATING FROM SCANNED IMAGES

The discussion in this appendix is not intended to, and should not be construed to, represent legal advice on this issue. Appropriate legal advice should be obtained from those professionally qualified to advise on these and related matters.

INTRODUCTION

One of the key questions that entities using EDM need to ensure is appropriately answered is "are our documents legal?" or "is digitally stored information admissible in a court of law?" After cost, the legal admissibility issue is the most asked question. In view of the lack of legal precedent in this area, entities should refer to appropriate laws of evidence in their jurisdiction and any relevant interpretations thereto. The purpose of this appendix is to discuss, in general, some of the issues that the entity and the auditor should be aware of. 1

It should also be noted that this discussion focuses on the imaging component of EDM. Many discussions contained in this appendix could, however, be applied to other electronic documents, for example, the discussion on computer-generated records in the section on the proposed Uniform Electronic Evidence Act. 2

EVIDENTIARY OBJECTIVES FOR IMAGES

Evidentiary Considerations for Imaging in Canada

The following are some of the issues that should be considered: 3

- The procedures and systems that comprise the program of records capture, storage, retrieval and fraud prevention should be fully integrated into the normal and ordinary course of the entity's business.
- There must be written authority by responsible officials for the regular destruction of the originals and that the prescribed program of destruction must be followed (see paragraph 9 below).

- A comprehensive system of quality assurance must be built into the imaging program to address the completeness of capture of all records received by the entity, the accuracy of capture of individual imaging transactions, the completeness of capture of all relevant features of a business record on the transaction, the authorization for the capturing of the business record, and the maintenance and preservation in unaltered form of the captured transaction.
- The imaging program must provide for the proper safeguarding of the media on which the transactions are stored.

Legal Admissibility

4 The legal admissibility issue is an important question. There are several issues to be addressed in this area, including:

- Have there been any court cases regarding optical storage?
- What factors are important to admittance?
- Can the paper original documents be destroyed?
- Will government agencies accept optically stored images?

There are a number of important considerations for answering these questions. These are specifically addressed in the sections that follow.

5 In general, court decisions for admissibility of evidence typically focus on the primary objectives of accuracy, reliability and trustworthiness. The storage media used for evidence have not affected the decisions. Technically, however, optical media should be admitted more readily than magnetic media, because information on certain types of optical storage cannot be easily altered.

6 The courts also may consider the enterprise's treatment of stored documents when considering admissibility. When enterprises routinely rely on stored documents when conducting day-to-day operations, it is reasonable to expect that the courts will consider them admissible.

7 Enterprises should develop procedures to ensure that documents are maintained in a legal form, which may sometimes necessitate documents being retained on paper or microfilm.

Audit Trails

8 The imaging system should operate in such a way that the application of basic and supervisory control techniques can be easily proved. Biographic data as to the system operation should be inherent to the operation of the image management program and automatically produced by it, otherwise operator certificates should be used and stored. In addition, all authorization functions should be traceable through controlled bibliographic and biographic information to specific individuals and equipment, operating as set out in the client's image management program.

Certifying Disposal of Source Records

9 Most of the photographic document provisions in the Evidence Acts require proof (which can be in the form of an affidavit or sworn declaration) that the source record was disposed of as a condition-precedent to the admissibility of a

print from photographic film. Although image-produced documents are not subject to these provisions, similar requirements might be imposed on them by means of judicial interpretations for other applicable statutory provisions (such as the business document provisions found in most, but not all, of the Evidence Acts, and/or the banking document provisions found in all of the Evidence Acts), or imposed by other rules of law (such as common law or judge-made law). Therefore, to provide evidence using image-produced documents, rather than source records, proof of disposal and replacement of the source records by means of a well regulated image management program will likely be required.

If paper source records must be kept for a designated period after capture, however, a separate record of disposal of the paper source records may have to be kept. The Evidence Acts do not specify retention periods for image-processed records as they do for microfilmed records. If they are disposed of before the fixed period, it is up to the courts to decide whether the microfilmed records can be used as evidence, rather than being admissible into evidence as of right. There is no comparable rule for electronic image-processed records. But, because of the vagueness and breadth of the language in the Evidence Acts that applies to business documents, comparable requirements could be imposed because of the broad scope of judicial interpretation that language could support. 10

ADMISSIBILITY ISSUES

United States

Background

A principal guide for the treatment and management of record copies is the Uniform Photographic Copies of Business and Public Records as Evidence Act (UPA). This uniform law applies to most public and private entities and to administrative and judicial proceedings. UPA applies to judicial or administrative proceedings under federal jurisdiction and has been adopted by some States. UPA indicates that the following record copies will be accepted as original records: 11

- Copies made in the regular course of business.
- Copies that accurately reproduce the original or are reproduced in a durable media.

Title 28, Section 1732 of the Federal Code adopts the principles of UPA and makes the following points concerning the use of copies. 12

- Copies must be made in the regular course of business.
- Copies must be an accurate reproduction or reproduced in a durable media.
- Copies produced from copies may be accepted as evidence.
- Original records may be destroyed, if destruction is performed in the regular course of business.

The customs of accepting business record copies as evidence may reside solely with the judiciary in the absence of explicit law; the entity should therefore find out if the state or the local authority has adopted statutes similar to UPA. 13

14 Another guide for the acceptance of record copies is provided by the Federal Rules of Evidence, Title 28, Unite States Code, Rule 1003, Admissibility of Duplicates. The rule indicates that a duplicate is admissible to the same extent as an original, *except* as follows:

- a genuine question is raised as to the authenticity of the original, or
- in the circumstances, it would be unfair to admit the duplicate in lieu of the original. Under this rule, copies may be produced by the same means as original records or via replication technology such as electrostatic or digitized copying machines.

Admissibility issues

15 Federal courts generally consider record copies as "hearsay." As stated in the Uniform Rules of Evidence, Rule 801 (c), "Hearsay is a statement other than one made by the declarant while testifying at the trial or hearing, offered in evidence to provide the truth of the matter asserted."

16 Because hearsay and (more specifically) record copies are not normally acceptable as evidence, courts have established a set of principles under which record copies are accepted. These rules apply to record copies used as evidence in Federal courts. States have also adopted versions of the Common Law Business Records Exception to the Hearsay Rule; records managers should examine the precise wording of these rules in their States. The range and scope of particular State rules are significantly different from State to State.

17 When record copies are admitted as evidence, it is incumbent on the records manager to demonstrate trustworthiness of both the record copies and the program practices used to maintain them. The trustworthiness of records systems is demonstrated by making record copies during the regular course of business and during or near the time of the event. Trustworthiness is enhanced when record copies are made by persons with knowledge of the event and are normally used in the entity's specific business activity.

Canada

Background

18 Again, because of the new nature of imaging, there have been no legal cases that have shed opinions on imaging and electronic evidence. As a result, there are various guides that might be used. These are discussed below.

19 In general, image capability has moved many entities to a totally paperless operation in many of their essential business functions. It has been stated that it is important for these entities to dispose of the original paper records. First, a large portion of the immediate financial benefits of implementing image are derived from the elimination of the sorting, filing and storage functions. Image users generally hold the paper for a short period of time to ensure that the captured image is legible. The paper is then shredded. Second, many entities are required to produce their business records in court or before a Regulatory Agency. If the paper original exists, it is considered to be the "best evidence," and, therefore, a copy such as an image or microfilm might not be admitted as

evidence unless the original is made available for comparison. The cost to these entities to find paper that has been chronologically filed over a period of years is often prohibitive. For these reasons, it is operationally imperative that the paper-based original records be destroyed shortly after their capture in the image system, and that there be proof readily available that the system has captured and can produce reliable copies of those originals.[1]

National Standard of Canada — Microfilm and Electronic Images as Documentary Evidence

This standard was developed by the Canadian General Standards Board in November 1993 and is intended to provide only general legal information and not legal advice. Some of the introductory highlights of the material are: 20

- Canadian law has yet to decide whether electronic images are either original computer-produced source records, or copies of source records. If originals, they would be subject to the same rules that apply to all other computer-produced records. Canadian law provides no detailed description of the evidence required to ensure that computer-produced records will be treated as credible when they are admitted into evidence in court. Therefore, each record or record-keeping system can have its own unique evidentiary problems.
- The image program must be part of the entity's "usual and ordinary course of business."
- The admissibility and credibility of image-produced copies cannot be equal to that of the source records without proper authority to dispose of source records and to keep the entity's permanent records on electronic or micrographic media.
- Copying, without disposal of source records, is merely the creation of another copy; it is not the creation of a new source record.
- It is necessary for an entity to have guidelines and procedures so that it can demonstrate to a court, etc., that it has a credible image management program capable of copying source records accurately, reliably and in a timely fashion without loss of value.
- At all times, the entity must be prepared to produce its imaged copies as evidence.

Some excerpts are set out in the paragraphs that follow.

> "A suggested list of specific points for proof when presenting computer-produced records as evidence is given in the explanatory notes (Part IV, par. 3.7). They are subject to being displaced if the law changes by providing its own list of points for proof, or a detailed description of required evidence. These points provide a method of demonstrating compliance with this standard's prime evidentiary requirement that at all times an entity must

[1] Taken from "Image and the law of Evidence — Implications for Business Processes," *Image Processing*, The Coopers & Lybrand Consulting Group (November 1991).

be prepared to produce its images as evidence. Therefore, they should be listed in the entity's procedures manual as a means for preparing testimonial and affidavit evidence with which to adduce computer-produced business records as evidence. The capture of biographical information should facilitate that preparation. These points provide a method of implementing this standard's evidentiary requirements in court.

"If in addition to, or instead of, the evidentiary requirements for computer-produced records, image-produced records are treated as being copies of source records (originals), the following additional points might apply. Generally, courts will accept a copy as a substitute for a source record if: 1) the source record is no longer available, 2) the copy was made with the intention of standing in the place of the source record, 3) the absence of the source record is adequately explained, and 4) the circumstances of disposal of the source record and the creation of the copy are adequately explained. Again, the application of these points will vary with the evidentiary problems presented by each record sought to be adduced into evidence, and with the specific legal rules that are applied to them. To go beyond these general statements to more specific statements requires professional legal advice because each record will have its own unique evidentiary problems.

"**Audit Trails** — The EDM system shall operate in such a way that the application of basic and supervisory control techniques can be easily proved. Biographic data as to the system operation must be inherent to the operation of the image management program and automatically produced by it, otherwise operator certificates must be used and stored.

"All authorization functions shall be traceable through controlled bibliographic and biographic information to specific individuals and equipment operating as prescribed in the image management program.

"**Supervisory Control Objectives** — The control techniques employed to satisfy control objectives in Part III, Section 3 shall be subject to additional supervisory control techniques to ensure their continued operation. Basic supervisory control requirements include:

- the appointment of an officer responsible for the integrity of the image management program, and
- the systematic supervision from image capture to disposition and storage.

"**Certificate of Disposal of Source Records** — Most of the photographic document provisions in the Evidence Acts require proof (which can be in the form of an affidavit or sworn declaration) that the source record was disposed of as a condition-precedent to the admissibility of a print from photographic film. Although image-produced documents are not subject to these provisions, similar requirements might be imposed upon them by means of judicial interpretations for other applicable statutory provisions (such as the business document provisions found in most but not all of the Evidence Acts, and/or the banking document provisions found in all of the Evidence Acts), or imposed by other rules of law (such as common law or judge-made law).

Therefore, to provide evidence using image-produced documents rather than source records, proof of disposal and replacement of the source records by means of a well-regulated image management program will be required.

"However, if paper source records are required to be kept for a designated period after capture, a separate record of disposal of the paper source records will have to be kept. There are no retention periods specified in the Evidence Acts for image-processed records as there are for microfilmed records. Most of the provincial Evidence Acts require that the source records that have been microfilmed be kept for a fixed period."

Proposed Uniform Electronic Evidence Act

At its annual meeting in 1994, the Uniform Law Conference of Canada adopted a set of principles to govern evidence of computer-generated records. Relevant excerpts are set out below. It should be noted that this material has not been enacted into statute at the present time. 21

Admissibility of data record

In a legal proceeding, nothing prevents the admission into evidence of information on the ground that it is in the form of a data record.

Original record

Information in the form of a data record has the same status in evidence as an original version of the information if the information is printed on paper or otherwise displayed in a way that accurately reproduces the information in its material form, whether it was first composed as a data record or otherwise.

Best Evidence Rule

18.11 Subject to this Act or any other Act of Parliament, production of the original is required in order to provide the contents of a record.

18.12 (1) A duplicate is admissible to the same extent as an original unless the court is satisfied that there is reason to doubt the authenticity of the original or the accuracy of the duplicate.

(2) Where an admissible duplicate cannot be produced by the exercise of reasonable diligence, a copy other than a duplicate is admissible in order to prove the contents of a record in the following cases:

(a) the original has been lost or destroyed;

(b) it is impossible, illegal or impracticable to produce the original;

(c) the original is in the possession or control of an adverse party who has neglected or refused to produce it, or is in the possession or control of a third person who cannot be compelled to produce it; or

(d) the original is a public record or is recorded or filed as required by law.

(3) Where an admissible copy cannot be produced by the exercise of reasonable diligence, other evidence may be given of the contents of a record.

Authentication

18.13 Subject to this Act or any other Act of Parliament, or exception provided by the common law, the proponent of a record has the burden of establishing its authenticity, which burden may be satisfied by the introduction of evidence capable of supporting a finding that the record is what its proponent claims it to be.

18.14 (1) Unless the court orders otherwise, no record produced by a computer system shall be admitted in evidence under this Part unless the proponent of the record has, at least seven days before its production in the legal proceeding, given to each of the other parties notice of his intention to produce the record and notice that the record was produced by a computer system, and has, within five days after receiving any notice requesting production of the record given by any such party, produced it for inspection by that party.

(2) Unless the court orders otherwise, production of the record in the form of a printout or other intelligible output of the computer system constitutes compliance with a notice given under subsection (1) to produce the record for inspection.

(3) Where the proponent of a record produced by a computer system has given notice to another party in accordance with subsection (1), proof of the authenticity of the record shall be deemed to have been waived by that party unless within five days after receiving the notice that party has filed with the court a notice requesting proof of the record's authenticity.

18.15 (1) The authenticity of a record produced by a computer system may be established by

(a) evidence that on comparison the record produced by the computer system corresponds in every material particular to the data supplied to that system; or

(b) evidence that the computer program used by the computer system to produce the record reliably processes data of the type in question and that there is no reasonable ground to believe that the correspondence between the record in question and the data supplied to that system has been adversely affected in any material particular by any process or procedure or by any malfunction, interference, disturbance or interruption.

(2) The court may require that evidence respecting the authenticity of a record produced by a computer system be given by a custodian of the record, or other qualified witness.

(3) Evidence of a custodian of the record, or other qualified witness, may be given by affidavit unless the court requires that it be given by way of testimony in court.

(4) Where evidence under subsection (3) is offered by affidavit,

(a) it is sufficient for a matter to be stated to the best of the knowledge and belief of the affiant; and

(b) it is not necessary to prove the signature of official character of the person making the affidavit if the official character of that person is set out in the body of the affidavit.

(5) The Governor in Council may make regulations respecting the form and contents of the affidavit referred to in subsection (3).

5. Subsection 30(1) of the said Act is repealed and the following substituted therefor:

30.(1) A record made in the usual and ordinary course of business is admissible whether or not any statement contained in it is hearsay or a statement of opinion, subject, in the case of opinion, to proof that the opinion was given in the usual and ordinary course of business.

GLOSSARY OF SELECTED TERMS

List of Abbreviations Used in this Study

AIIM	Association for Information and Image Management
API	Application programming interface
ASCII	American Standard Code for Information Interchange
CALS	Continuous acquisition and life-cycle support
CGM	Computer graphics metafile
COLD	Computer output to laser disk
CRC	Cyclical redundancy checks
ICR	Intelligent character recognition
JPEG	Joint Photographic Experts Group
LAN	Local area network
MPEG	Moving Pictures Expert Group
OCR	Optical character recognition
RAID	Either redundant array of inexpensive devices or redundant array of independent devices
SQL	Structured query language
TIFF	Tagged Image File Format
WAN	Wide area network

Admissibility
"Admissibility" and "admitted into evidence" refer to the acceptance into evidence by a judge in judicial proceedings, or by the presiding officer at a tribunal or public or formal inquiry, of documentation or information that is produced at such proceedings, tribunal or inquiry.

Algorithm
A set of mathematical steps used to compress image files or other operation in a computer.

Alphanumeric
A characters set that includes letters and numbers and may include punctuation.

American Standard Code for Information Interchange
A 128-character, seven-bit code for data transfer adopted by the American Standards Association to achieve compatibility between data devices.

Analog
Opposite of digital information. It means record of data into electronic representations that are based on tones or magnetic current.

Annotation
An addition to the content of the image of the original, generally made by the entity itself. Annotations do not alter the source record.

Application
Any computer program that executes commands for the computer system.

Application Programming Interface
Consists of a series of programming variables that can be used to enable programmers to write programs or utilities that gain access to external programs or utilities.

Association for Information and Image Management
A group devoted to establishing imaging standards and disseminating information to the imaging community.

Asymmetrical
Used to describe the type of compression used by many compression systems. It takes an equal amount of time to compress and uncompress the file. See Symmetrical.

Authoring Tools
Industry standard term for electronic tools used to create a document.

Automated Retrieval
A system that assists in retrieving images using an index and software tools for the user.

Average Access Time
The average amount of time it takes to find a specific piece of data on a storage system.

Backfile Conversion
The process of converting paper documents created before the installation of document imaging to an electronic format.

Basic Control Techniques
The techniques that ensure the integrity of the image management program and the systematic supervision of image capture to disposition and storage.

Batch Processing
Performing several operations at the same time. Hundreds or thousands of documents can be scanned together in a batch and then assigned to folders later.

Biographic Information Part of the Index
Information contained within an index created by the entity that describes particular attributes of the document that are of interest to the entity: (for example, may include date & time captured, operator identification, capture device identification, location, details of modification).

Bit-mapped Image
Data from a document represented in digital form by assigning each recordable piece of information to a unique memory location.

Blocking
The adhesion of two or more documents to one another.

Boolean Logic
A system for representing set relationships using AND, OR and NOT operators.

Browsing
The process of finding a piece of image information in a data base that is not present in the index.

Cache Memory
(Mainframe) a high speed memory used as a buffer between the central processing unit (CPU) and main memory, it is used to store sequences of instructions from main memory.

(Microcomputer) a very fast section of random access memory (RAM) set aside to store the most frequently accessed information stored in RAM.

Capture
The creation of an image from a source record.

CD-ROM
Media, in the form of plastic disks, for storing and playing back computer data, audio and video information. These disks are permanent storage and data will not be lost unless the disk is physically damaged. Their small size (under 5") is compact and easy to store.

Certificate of Image Authorization
This certificate authorizes the image capture and commitment of the images to secure storage in accordance with the entitys policy to keep a permanent record thereof. It should include the date, name of authorizing person and sufficient biographical information to clearly identify the records. This certificate may be

a paper document (kept separately), an electronic image or an electronic record stored within the boundaries of secure storage.

Character Recognition
Optical Character Recognition (OCR) or Handprint Character Recognition (HCR) processes in which handwritten characters are read and converted to their ASCII equivalent.

Compression
A method of reducing the size of the document image by performing transforming data bits into patterns that can be stored in a much smaller space.

Computer Graphics Metafile
A graphic format for storing document images or other types of graphics.

Computer Output to Laser Disk
The method of writing image data to a laser disk and retrieving them using a separate subsystem for fast output to optical storage.

Continuous Acquisition and Life-cycle Support
US Department initiative (1985) to provide a framework for the transmission and usage of information on weapon systems in electronic form. Support for this initiative led to adoption of standards such as Standard Graphic Markup Language (SGML).

Cyclical Redundancy Checks
A calculation that compares two different pieces of data to determine if they are identical.

Data Compression
The process of converting black, white and grayscale images to an encoded form to reduce optical storage requirements.

Decompression
The process of converting images from a compressed format so they can be viewed on a monitor or printed. It reverses the original compression by taking the formulas and creating image information for each location on the screen.

Defect Distribution
The measurement of the track and radial defects present in the optical storage media.

Defect Management
The method for writing and reading information from/to the optical media despite defects. The process uses programs to detect and manage the placement and interpretation of data.

Digital
The use of binary code to record data in a computer. The values of 1 and 0 are represented by the presence or absence of a voltage.

Digital Image
The binary representation of document information employing computer and communications technologies.

Digital Scanner
Hardware for converting variations in contrasting colour on documents to binary data.

Disposal
The destruction, erasure, loss or delivery out of the entity of a source record in the ordinary course of business.

Document
Data organized into a logical order and preserved on a media (for example, disk, paper, etc.).

Document Imaging
The processing of converting paper-based documents to an electronic format and then storing those images and viewing them on a computer monitor as needed.

Document Readers
Specialized scanners that perform Optical Character Recognition on document images.

Document Retrieval System
Computer assisted program for users to request the viewing or printing of documents stored as images. See also Print-On-Demand Systems.

Document Sampling
The viewing of documents on a random or subjective basis for the purpose of auditing or verifying document integrity.

Electronic Image
The storage of images on disk or tape as a series of 1 and 0 bits.

Electronic Imaging
The capture, storage and display of electronic images.

Encryption
A technique for protecting information within a computer system, on magnetic media or during transmission. An algorithm transforms the data to render them unintelligible. The process can be reversed to regenerate the original data for further processing.

Erasure
Removal of image related information so that no one can become aware of the deleted record through any automated or manual mechanisms used in the normal course of business.

Evidence
That body of testimony, documentation and physical objects that will be "admitted into evidence" by a court or tribunal as a proper source for determining facts and making decisions.

File Server
The central computer on an local area network where all of the shared data and programs are stored.

Filtering
A method used in document imaging to clean up documents for extraneous spots or other problems.

Firewall
An electronic device that, by not permitting network traffic to pass through it, separates or isolates a network segment from the main network; a connection between networks is, however, maintained.

Fourth Generation Programming Language
A high-level programming language that offers direct control over hardware devices.

Full Text Search
Searching text files for the occurrence of any words or punctuation inside the text. All works are searchable rather than just keywords.

Graphical User Interface
A software standard used for displaying information on the computer monitor in a graphical versus a text format.

Hierarchical Storage Management
A method of storage that moves data from magnetic disks to optical disks to tape automatically.

Image Enabling Software
Software that converts standard databases into image storage capability. This enables databases that may already be in use by entities to be used for imaging.

Image Management Program
An authorized program following strict control guidelines to achieve specific objectives in the capture, storage, and retrieval of images. This may also include the disposal of source records.

Image Management System
A system of procedures and technological components that operate in an integrated manner to capture, store, index, retrieve, distribute, insert, erase and modify images.

Image
The representation of a record that can be used to generate an intelligible reproduction of that record, or the reproduction itself, where: (a) the reproduction was made with the intention of standing in place of the original, (b) the interpretation of the reproduction, for the purposes for which it is being used, yields the same data and information as the source record, (c) the limitations of the reproduction (for example, resolution, tonal or hues) are well defined and do not obscure significant details.

Image Acceptance Sampling
The task of sampling a set of images to determine the quality of the image. This task may be performed as part of an audit or as a regular quality assurance program.

Image Conversion
The process of converting paper documents to bit-mapped data.

Index
A method of identifying document images by assigning a word or words to each image so that the computer can search for desired images.

Intelligent Character Recognition
Software enabling an Optical Character Recognition process to enhance recognition capabilities by learning rules within a context. A proprietary method of character recognition from scanned images that uses artificial intelligence for a high level of accuracy.

International Standards Organization
An entity that creates standards for a variety of systems. Its work includes computer system standards (for example, the CD-ROM IS0-9660 standard.)

Joint Photographic Experts Group
A standard for compression that is widely used in document imaging.

Jukeboxes
Commonly used with optical disks where a number of disks are stored in the rack and two or more disk drives are used to access the disks. The disks are moved in and out of the drives automatically by robotic arms.

Keywords
Linking a word or phrase with images so a computer search can be performed to find the desired image. Since data inside the form cannot be searched by the computer, these external values automatically linked to the image make searching easy.

Legacy Systems
Mainframe business software systems, such as, for example, bank finance systems that were developed using the technology of the 1970s to mid-1980s.

Local Area Network
A communication system where a number of computer systems are on the same high performance wiring system.

Local Area Network Protocol
The method used to communicate on a local area network. These protocols specify how data are transmitted and received.

Magneto-optical Drive
Storage media composed of magnetic materials, but written to using a laser. The laser does not change the media's physical properties; only the polarity is changed. Unlike the write-once-read-many drive, data stored on this medium can be changed.

Moving Pictures Expert Group
A compression standard designed for moving images, such as video, proposed by an ISO committee of the same name.

Object-oriented Programming Language
A nonprocedural program language in which program elements are conceptualized as objects that can pass messages to each other.

On-line Storage
A method of storing data that is automated but not constantly on-line. Frequently a jukebox is used (see Jukebox.)

Operator Capture Certificate
A document that confirms the image capture of a source document by personnel authorized to input documents into a given Image Management System.

Optical Character Recognition
A system to scan document images and convert images of characters into computer text.

Optical Character Recognition Indexing
The automated creation of the document's index by the system's ability to recognize and use information on the document.

Optical Storage
A medium requiring lasers to permanently alter the physical medium which creates a permanent record. The storage also requires lasers to read stored information from the media.

Quality Assured Image Record
Set of quality assured images, which has associated index data (for example, bibliographic and biographic) and the linkage between the image and the associated index data, that have been verified according to quality assurance procedures and maintained in a manner that provides confidence that the image can be retrieved, therefore allowing it to stand in place of the source record.

Query
In database management programs, a search question that tells the program what kind of data should be retrieved from the database.

Query by Example
In database management programs, the ability to submit an existing body of text as a full-text query.

Query by Form
In database management programs, a query technique that prompts the user to input the search criteria into a template resembling the data record. Query construction is facilitated through the use of "fill-in the blank" screens and menus.

Query Language
A defined set of commands and syntax used to submit queries to a text retrieval system.

Redundant Array of Inexpensive Devices or
Redundant Array of Independent Devices
An array consists of several disk drives where data are spread across the drives in a manner that the removal of any one drive means no loss of data. If one drive fails and is replaced by a new one, the other drives will copy the relevant data to the new drive. All of this can be done while users are accessing data on the system.

Raster Graphics
Computer images. Digital pictures stores as a series of zeros and ones; a bit map.

Relational Databases
Databases that consist of separate tables to store related information. This is a very efficient method of storing and retrieving information. Used extensively in document imaging systems.

Rewritable Optical Disks
A type of optical disk where data can be recorded, modified and erased. Standard types of optical disk make a permanent copy of data that cannot be changed.

Scanning
The processing of taking a "picture" of a paper document and converting it into an electronic format.

Secure Storage
The storage repositories used to hold quality assured image records during the retention period, in a manner that satisfies various the control objectives.

Source Record
(a) In relation to a record, the record itself or any facsimile intended by the author of the record to have the same effect, (b) in relation to a record produced by a computer system, any printout or other intelligible output that accurately reproduces, whether in the same or a modified form, the data supplied to the computer system.

Structured Query Language
A standard method of creating queries of the database that will yield desired answers. Used with client/server databases.

Supervisory Control Techniques
Procedures undertaken by the entity that ensure that the basic control techniques prescribed in its image management program are consistently and effectively applied.

Symmetrical Compression
Techniques that take the same amount of time to compress and uncompress. See Asymmetrical.

Text Annotation
Creating text comments connected to a document image. These comments can include authorizations or reaction from users.

Tagged Image File Format
A graphical format for storing images on disk. The most popular file format in document imaging.

Transitional Storage
Storage repositories used to hold image and related data records, other than in secure storage.

Wide Area Network
A local area network that is geographically dispersed over a large area.

Workflow
Software programs that incorporate document imaging but also provide routing and automation functions.

SELECTED BIBLIOGRAPHY

American Institute of Certified Public Accountants, Proposed Statement on Auditing Standards No. 80, "Amendment to Statement on Auditing Standards No. 31, Evidential Matter" (December 1996).

Arend, M., "Check Imaging: Banks are getting the picture," *ABA Banking Journal* (May 1992).

Bennett, J.C., "Audit and Control Issues of Image Processing," *Computer Audit Update* (Elsevier Science Publishers Ltd., March 1992).

Berry, M.D., *Document and Image Management,* Patricia Seybold Group Incorporated (Boston, Mass.: January 1995).

Bogusky, C. and Halper, S., "Control and Security Issues in Electronic Document Management Systems," *The EDP Auditor Journal* (1991-Vol. IV).

Brown, A.E., "Imaging Advances Competitive Edge", *IMC Journal* (May/June 1994).

Burke, M., "Moving a document mountain," *Hum — The Government Computer Magazine* (1995).

Canadian General Standards Board, *Microfilm and Electronic Images as Documentary Evidence* (Ottawa, CGSB, 1993).

Cinnamon, B., "Justifying Image Processing Systems," IMC *Journal* (September/October 1990).

Croop, D.L., "Insurance Image Management: A "Hybrid" Solution," *IMC Journal* (March/April 1993).

Data-Tech Institute, "Understanding Document Imaging," (1995).

Emerson, J., "French Insurer Uses Imaging to Cut Business Risks," *Inform* (April 1996).

Etherington, A., "The DIP Alternative," *Accountancy* (February 1995).

Francis, T. "Image Capture Means Freedom from Paper," *Bank Administration* (September 1988).

Fry, R.B., "X Marks The Spot: New Technologies Compel New Concepts for Commercial Law," *Loyola Of Los Angeles Law Review* (Volume 26 , April 1993, Number 3).

Gant, J.J., "Work Management: The Next Step in Imaging," *Chief Information Officer Journal* (Fall 1992).

Gartner Group, *Functional and Technical Requirements of an Imaging Program* (September 25, 1995).

Geer, T. and Hickey, T., "Catch the Image-Processing Wave," *The Bankers Magazine* (January/February 1991).

Global Concepts Inc., A Financial Industries White Paper "Managing the Future With Image Technology," (1994).

Hall, G.M., "It Always Looks Easy from the Bridge," *Inform* (April 1994).

ISO *Electronic Imaging — Legal Considerations for Storage Media in Record Keeping,* Draft Version 1.0 (February 28, 1994).

Kakhsaz, A.R., "Getting the Picture on Document Image Management," *Journal of Accountancy* (December 1991).

Koulopoulos, T.M. and Frappaolo, C, *Electronic Document Management Systems — A Portable Consultant* (McGraw Hill Inc., 1995).

Lucia, B., "Innovative Technology Results in Superior Customer Service and Reduced Costs," *IMC Journal* (May/June 1994).

Meall, L. and Price, A., "Conquering the Paper Mountain," *Accountancy* (November 1993).

Parker, J.W., "Herzog Plays The Jukebox," *Wall Street & Technology* (Volume 12, No.3).

Plagman, B.K. and Littlejohn, M.V., "Control and Audit of Electronic Document Image Processing ," *Price Waterhouse* (1992).

Plagman, B.K. and Littlejohn, M.V., "Image Processing," *Internal Auditor* (December 1992).

Radding, A., "Is Your Image Legal?" *The Federal Credit Union* (March/April 1992).

Ristuccia, H.J. Saia, C.A., "Control, Auditibility and Recoverability of Optical Storage," *IS Audit & Control Journal* (Volume V, 1995).

Ristuccia, H.J., "Imaging Systems: Security, Control and Recoverability," notes from *Computer Security Institute* 22nd Annual Computer Security Conference & Exhibition.

Schantz, H.F., "OCR-Enhanced Electronic Image Management Systems Minimize Operating Costs," *Document Image Automation* (Fall 1992).

Scott, R., "Workflow Dundee," *Inform* (October 1994).

Shegda, K.M. and Richardson, M.A., "Document Imaging Systems and Software: Overview — Market Analysis," *Datapro Computer Systems Analyst* (McGraw Hill Inc., December 1993).

Shegda, K.M., "Document Imaging Systems and Software: Overview — Technology Analysis," *Datapro Computer Systems Analyst* (McGraw Hill Inc., September 1995).

Smith, C.R., "Opting for Optical," *Wall Street & Technology* (Volume 11, No. 10).

Starbird, R.W. and Vilhauer, G.V., "A Manager's Guide to Electronic Imaging" (Association for Information and Image Management, 1993).

Sullivan, R., "Underwriter Tracks Policies in Record Time," *Inform* (April 1996).

Systems Auditability and Control (SAC) (Alamonte Springs, Fla: The Institute of Internal Auditors Research Foundation, 1991).

The Coopers & Lybrand Consulting Group, *Image Processing* (November 1991).

The Document Management Guide, (Waltham, Mass.: Interleaf, Inc., 1994).

Thé, L., "Workflow Tackles the Productivity Paradox," *Datamation* (August 15, 1995).

Thode, J.P. and Vanacore, M.E., "Security and Control of Imaging Systems," *Data Security Management* (1995).

Trowbridge, D., "Imagine A Notary Stamp for Electronic Documents," *Computer Technology Review* (Volume XV Number 4, April 1995).

Uniform Law Conference of Canada, *Proposals for a Uniform Electronic Evidence Act May 30, 1995.*

United States General Accounting Office, *Assessing the Reliability of Computer-Processed Data* (Washington, D.C.: GAO, September 1990).

Vecchione, A. "Imaging's Healthy Reflection," *Information Week* (June 22, 1992).

Walpole, D. "Imaging Wends Way Through Whole Bank," *Bank Technology News* (July 1994).

Walton, S., "Image authentication for a slippery new age; knowing when images have been changed," *Computer Select* (September 1995).

Williams, R.F., "Electronic Document Management: The Coming Revolution in Records Management," *IMC Journal,* International Information Management Congress — Special Report.

Williams, R.F., "Imaging and the Law," *Chief Information Officer Journal* (May/June 1993).

Williams, R.F., *Legality of Optical Storage — Admissibility in Evidence of Optically Stored Records* (Chicago, Ill.: Cohasset Associates, Inc., 1994).

West, A., "Pacific Mutual Life Puts a Premium on Workflow," *Inform* (April 1996).