Payoff

Not all electronic image management systems are the same; they come in a variety of shapes and sizes. They may be implemented as integrated additions to an existing technology architecture or as a standalone system. The potential security risks vary with the environment and as a function of the application. This article presents an overview of electronic imaging technology and typical imaging applications that may be found in business today. It then describes security and control issues that must be addressed in these systems and applications.

Problems Addressed

Electronic image management (EIM) systems are used to store and retrieve information as well as provide an integral part of automating operational procedures. The benefits of storing and retrieving documents on Electronic Image Management systems include:

- A reduction in space required to store documents and associated cost savings related to managing the files.
- Enhanced operational efficiencies achieved through increased document accessibility.
- Simultaneous access to imaged documents by multiple users and a significant reduction in the time necessary to retrieve documents.

Using EIM to automate work flows can result in operational efficiencies and enhanced accuracy and completeness of work performed. For example, insurance companies typically microfilm a claim when received and then circulate the claim form paper document to various personnel or departments until it is adjudicated. However, with EIM technology, insurance companies can scan a claim form, create an electronic image, and electronically transmit the image to a claims examiner for entry into the claims system. Selective fields are automatically input from the claims form to the claims entry screen using Optical Character Recognition. Using EIM systems to process claims has directly resulted in reduced time and increased accuracy in processing claims. Other examples of EIM applications include mortgage processing, accounts payable, processing and rating bills of lading, litigation support, and trademark and patent storage.

EIM technology can have an impact on the integrity, validity, and completeness of processed information. Companies using EIM systems to store documents needed for business and legal requirements or as a method to initiate transactions need to ensure that such information is protected from unauthorized destruction or modification. In addition, confidential and sensitive electronic images must be protected from unauthorized viewing and disclosure. As the use of EIM technology increases, the impact of such technology on the overall security and control environment will also increase.

It is often difficult to describe the imaging system security and controls environment that is needed. It is not always clear what the nature of the EIM system is, what the nature of the application is, or what processing strategy the application and system uses. Readers may also have different levels of experience and understanding of Electronic Image Management systems. Therefore, this article begins with an overview of imaging technology, imaging applications, and industry trends to help frame the environment which
is being reviewed. Information from the security and control sections of this article can be used to customize an approach for performing a security review and assessment.

**Overview of Imaging Technology**

EIM system components can be grouped in two ways. They can be grouped by the size of the hardware platform they run on—from mainframe computers to minicomputers and microcomputer systems—or by the function of the device type. A given device can be used for inputting and outputting images or moving and storing the images. Exhibits 1 and 2 provide examples of two types of configurations. Exhibit 1 presents a mainframe or minicomputer-based imaging system; Exhibit 2 presents a LAN-based client/server Electronic Image Management system. This section describes the components, grouping the devices according to function.

**Mainframe- or Minicomputer-based Electronic Imaging System**

**LAN-Based Electronic Imaging System**

It should be noted that most of the components of an electronic imaging system are not unique to imaging. EIM systems have integrated standard workstations, printers, and networks with scanners and optical disk systems to provide the capability to electronically process documents. Because much of the Electronic Image Management system is comprised of standard components, many of the security and control techniques that apply to securing centralized or distributed computing systems also apply to EIM systems.

**Input Devices**

Images can be entered in a variety of ways. Typically the source of the input is paper and the paper is input through a scanner. The underlying technology of scanners is similar to that of fax machines; however, certain scanner features are very different from those of faxes.

Scanners can process images at a variety of speeds from 1 page per minute to as many as 180 pages per minute. Various sizes of paper can be scanned, from 4frac12;” * 5frac12;” to large, blueprint drawings.

Scanning resolution, defined as the number of dots per inch that is scanned, is selectable at the scanner device. Resolution can vary from 100 to as many as 600 dots per inch. As the scanner resolution is increased, the resulting image contains more dots per inch and the image becomes clearer. The image also contains a larger number of bytes, which increases transfer time and storage space. Other features include the ability to scan both sides of a document with one pass through the scanner and to scan microfilm.

Some scanners also have the ability to decipher and recognize characters using Optical Character Recognition and Intelligent Character Recognition techniques. Optical character recognition is the ability to identify machine generated characters, usually printed in a single font and type size. Intelligent Character Recognition is the ability to identify a variety of machine-generated character font and type sizes as well as handwritten characters. Intelligent character recognition (ICR) algorithms can also potentially correct known errors or determine unreadable characters through field or character associations. For example, if the first character in a zip code was not readable in an address, an intelligent character recognition (ICR) algorithm may be programmed to look at the state in the address and determine the first character from the state.
Images can also be entered into an imaging system using a fax machine as the input device. This technique is typically used when inputs come from a variety of remote places, and the volume from any one location is relatively low. Transmitting documents from one imaging system to another is also sometimes accomplished using fax technology. One imaging system can send a document image formatted as a fax to another imaging system. Although the standards for internally representing or storing images may differ among imaging systems, a facsimile format is usually an acceptable input format.

**Storage Devices**

Imaging systems use a variety of storage techniques. Although many people associate imaging systems with optical disks, the storage media is independent of the imaging system. The type of storage device associated with a particular imaging system is a function of the volume of documents, the application's performance requirements, and the user's budget. For example, storing and retrieving images directly to or from optical disk can be time-consuming because of the large number of bytes per image and the rather slow write and read times of optical disk. Therefore, if there is a need to process or access a large number of documents in a short period of time, some imaging applications first store images on magnetic disk. Over time, as documents are required less frequently, the application may archive the images onto optical disks.

A collection of optical disk platters can be stored in a device called a juke box, as shown in Exhibit 3. A juke box can hold in up to 128 optical disk platters, and multiple juke boxes can be linked together. A juke box usually contains three components: storage space for the optical disk platters; robotic mechanisms which select a specific platter and place it in on a drive; and the drives themselves, where the optical disk platters are written and read. Optical disks are frequently populated using write-once-read-many (worm) technology. This means that data is permanently written onto the disk and the disks cannot be erased. Although erasable optical disks are beginning to appear more frequently in EIM systems, most existing applications still use worm technology to encode the data onto the optical disks.

**Juke Box Components**

Optical disks have a wide range of capacities and can store from two gigabyte to as many as ten gigabyte of information. For example, a twelve-inch optical disk platter with a two gigabytes capacity can store the documents that are contained in four four-drawer file cabinets. A juke box of 128 platters can store documents from 400 four-drawer file cabinets. Storage technology continues to improve and each year the capacity of these devices increases.

**Communication Networks**

All multiuser EIM systems are tied together through a communications network. The type of network depends completely on the application requirements, the location of the users, and whether information from other hardware platforms needs to integrate with the EIM system. Network communications design is critical to system performance, because the amount of information required for a bit-mapped image can be several orders of magnitude greater than information transmitted in character mode.
**Workstations and Printers**

EIM workstations are similar to most computer workstations, although large screens (e.g., 20-inch screens) are frequently used. This allows users to view the front and back of a document at the same time or to view multiple windows when more than one application is simultaneously processing. The resolution capabilities of the workstations should match the resolution level being used by the scanner. Without a proper match, the benefits of higher resolution images are lost, but the cost of managing and storing the additional information remains.

Most EIM systems use laser printer, because the output images are bit mapped. Although most EIM systems are designed to avoid use of paper, all systems include printers.

**EIM System Security**

In designing and implementing a security program for EIM systems, the following control areas should be evaluated:

- Destruction of stored documents.
- Validity of documents stored on the system.
- Availability of stored documents.
- Authorized use and viewing of stored documents.

There are costs associated with establishing a security program; therefore, the level of security required should be in balance with the criticality of the information to be stored and protected. In addition to business issues, legal issues should also be considered. For example, different processing and security for documents might be required should a suit be filed. The best course of action is to coordinate all legal issues with the organization's general counsel. The enterprise should also understand its position and exposure regarding the admissibility of electronic images in a court of law. It should also be noted that companies approach the legal aspects of imaging documents differently. Some companies in the same industry and application area have policies with respect to document access or archival storage of original documents that are diametrically opposed.

Electronic images can be secured through a combination of physical security, system access control software, and application access controls. As described, Electronic Image Management systems can reside on a mainframe, minicomputer, or LAN-based hardware platform. The access controls may be used in a variety of combinations according to the platform on which the Electronic Image Management system resides. For example, a user may have to log on to the system to gain access to the imaging system. This would be a system access control. Next, during the user session, in order to execute a particular transaction in an imaging system application, users may have to be authorized in advance or enter a password to establish that they have the authority to execute the transaction. This would be an example of an application access control. Of course, the terminals themselves could actually be secured in an area that requires a code to enter. This would be an example of physical controls.
Physical Security Controls

Comprehensive physical security measures can help ensure that only authorized users can scan and retrieve electronic images and that such images are protected from deletion or destruction. At a minimum, EIM hardware and related physical file storage devices need to be physically secured. In addition, it may also be important to physically secure document scanners by placing them in secured rooms to help ensure that only authorized documents are entered into the system. This may also be true for workstations, to help ensure that only authorized users can access images. The cost of EIM equipment, and its susceptibility to theft, should also be considered when designing physical security controls.

Logical Security Controls

Logical security is composed of access control security software, operating system software security (including security for data base and files), and application level security. Logical security controls allow the security administrator to:

- Restrict users from accessing unauthorized functions.
- Protect stored images from unauthorized modification.
- Secure documents from unauthorized deletion.
- Establish individual accountability for processed transactions.

Restricting system functions is important when the nature of the application requires duties to be segregated within an EIM application or if multiple EIM applications reside on a single hardware system. For example, an Electronic Image Management system which processes accounts payable transactions might segregate the three processes of scanning an invoice, retrieving and approving an invoice, and retrieving and inputting a payment transaction. This could help prevent the initiation of fraudulent payments and ensure the accuracy of input transactions. If multiple EIM applications process 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 the same system that 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 or system controls that manage and authorize access to data and application transactions.

Because of the nature of EIM technology, it is difficult to directly modify the contents of a document image. However, images are stored and retrieved using a data base index reference pointer. It is important to secure the index files in an EIM system.

A modified version of a document could be scanned into the system and the index reference pointer could be altered to point to the revised image. Unless some change control tracking is performed, the original image would be lost and the revised image would appear to be the original copy.

In addition, the index files must be protected to prevent the destruction or unauthorized deletion of documents. When an index is lost or altered, the pointer to the document is also lost or altered. The result is that the document is, in effect, deleted. Index files are generally created using relational data bases; they can be secured from direct access through the features available from the data base management system.

The ability to identify who has entered a transaction or scanned a document into the system can be important in measuring performance as well as identifying the perpetrator of a fraud. Access control systems as well as image system functions can be used to establish individual accountability for transactions processed. For example, in a scanning operation,
the system can ask the scanning operator for an ID number at the start of the operation to ensure that the operator is authorized to perform the required functions. After authorization is granted, the system can append this ID to each document as it is scanned. At a later time, if there is a need to identify the operator who scanned a particular document, the ID information appended to the document can be referenced.

**Input and Processing Controls**

In addition to establishing a secure environment through physical and logical controls, input and processing controls must also be designed into the Electronic Image Management application and related procedures to ensure the accuracy and completeness of EIM Transaction Processing. These include controls for document preparation, scanning, indexing, and transaction management.

**Document Preparation**

Input procedures include sorting and batching documents before scanning. This helps establish document and page counts and ensure that all documents are completely entered into the system. For example, in a mortgage processing application, such document types as mortgage applications, credit documents, and property-related documents could be separated. A count for each type of document could be used as a control total. As the documents are scanned into the system, the system would report the number of documents of each type it recognized; these could then be matched and verified to ensure that all documents are accounted for.

**Scanning**

As documents are scanned, controls to detect and correct problems and to ensure that documents are completely scanned should be established. This procedure could include a quality control step to view a scanned document to determine if a document had been missed or was incomplete, or if the quality of the scanned document was poor and the document was not readable. If these conditions existed, the document would need to be rescanned. It should be noted, however, that when documents are viewed during the scanning process, system performance will be affected. This review step may need to be separate from the scanning activity if high performance scanning is required. In environments in which procedures call for the destruction of original documents after the input process, the quality control process is very critical because the only evidential matter for business or legal purposes is the electronic image.

**Indexing**

If an error is made when a document is indexed, the document may not be accessible because the pointer associated with it is incorrect. If indexing is performed in a manual data entry step, it may be appropriate to have duplicate indexing activities. The activity is similar to key data entry procedures in which one operator enters the document index and a second operator reenters the index in a verification mode. The two entries are then compared by the system and correction procedures executed if the indexes do not match. If indexes are created by reading characters or bar codes from the document, a statistical sample of documents may be selected and reviewed at a quality control step to ensure that the automated process is accurate. All procedures should be designed to prevent the storing of partial documents and to ensure that referential integrity is maintained.
Transaction Management.

After a document is stored, procedures for access and use take effect. In procedural or work flow applications, security and controls must be in place to ensure that documents are routed to authorized users. Two types of work flow processing are found in EIM systems: “push” and “pull.” In a push-type system, the documents are automatically routed to the operators using the information described in the routing files. Users don’t usually have to request work, it just arrives at their workstations. In a pull-type system, users have to request each piece of work. They may also have some discretion about which work they request.

In a push-type system, a routing function can help control the documents being routed to authorized users. In many EIM systems, managing the routing files is usually performed by the system administrator and is usually a secure function. In some environments, document routing may be changed dynamically by the system to balance workload or manually at a supervisor’s discretion to initiate exception processing. Passwords should restrict authorization to change work flow routings to approved supervisors only.

In a pull-type system, routing controls can be managed on the basis of user skill sets of functions. Users are assigned a set of skills or a group of processes which they are trained to perform. When work is requested by a user and a document waiting for a particular process matches an operator’s skill set, the document is sent to that operator’s workstation. If the operator is not skilled in the particular process, no document would appear. Work routing can be changed in this case by altering the particular skill sets or authorized processes of each operator or group of operators.

Other security control features include monitoring and reporting document status to ensure timely processing, system throughput statistics, and operator activities. The latter might be measured in terms of the number of transactions processed, the average elapsed time a transaction stays at a work step, the number of transactions that are passed to a supervisor, or the number of transactions that are pending at the operator’s work step. Such performance measures as the que lengths of the various work steps may help indicate where operators need to be added or removed from a processing step.

Recovery Issues

The impact of using Electronic Image Management technology must be considered when establishing a business recovery strategy. The recovery strategy may require short-term recovery of computer systems or manual processing until the computer system is restored. Even if the recovery strategy is manual, the impact of EIM systems must be considered. For example, if the recovery strategy is to process manually until the computer system becomes operational, and the process uses EIM, the retention, storage, and retrieval of original documents becomes critical to the recovery strategy. A benefit of EIM in recovery planning is that it provides a cost-effective approach to backing up critical documents.

Recommended Course of Action

In order to establish an adequate security and control environment for an Electronic Image Management system, the security administrator should:

- Identify and document the complete Electronic Image Management technical environment. Because EIM systems can run on a variety of hardware platforms, knowing the complete technical environment helps ensure that the control tools best suited for a particular area are used.

- Identify the security and control objectives and business risks. Because security controls cost money to implement, it is important to understand the objectives and
business risks so that the cost can be presented in conjunction with appropriate benefits.

- Use a combination of application, system software, network, and user procedural controls.

- Ensure that certain practices are valid and feasible in an EIM environment. For example, making a backup of an optical disk platter may seem like a good idea. However, it can take up to 24 hours to complete a copy. Because of the large number of bytes of information EIM systems contain, certain traditional data processing procedures are not reasonable.

EIM can provide cost savings related to document storage and retrieval through decreased storage space, decreased file maintenance support, fewer out-of-file conditions, more complete files, simultaneous document access, and reduced document copying. However, businesses must consider governmental and regulatory requirements when considering EIM. Current laws generally accept electronic images when they are created as a result of normal, documented business procedures. Nonetheless, legal counsel should be consulted to ensure the organization is complying with current laws and regulations as well as its own corporate policies.

Author Biographies

Jerome P. Thode
Jerome P. Thode is a principal in the information technology practice of Deloitte & Touche in Los Angeles. He has more than 22 years of experience in IS strategic planning, systems development, and the planning and implementation of electronic image management systems.

Maureen E. Vanacore
Maureen E. Vanacore is a partner in the Deloitte & Touche Computer Assurance Services Group. She assists clients in assessing, designing, and implementing security and controls in systems, developing business resumption plans, and establishing internal EDP audit functions.