

Issue 1

The Legal Admissibility of Electronic Documents

An Executive Briefing Paper

Abstract	2		
Introduction	3	Admissibility and Rules of Evidence	15
Required System Characteristics	4	Sources & Acknowledgements	18

Abstract

Government, Industry and Commerce have moved firmly into the 'electronic trading' age. Electronic documents now form the basis for many business transactions and are produced, stored and transmitted in large numbers around the Globe. It is now possible to negotiate, sign for and deliver the services associated with a contract entirely over the Internet.

However, this raises some interesting points with regard to the admissibility of electronically held documents. Historically, documents were on paper and providing their provenance or integrity was demonstrated they were acceptable legally. Where a document is created or captured electronically concerns have been raised regarding how acceptable such electronic documents are.

This paper presents a picture of some of the processes and practices which are deemed to satisfy the various legal requirements. It uses illustrations based on current practice and guidance in use around the world.

Document and Content Management (D&CM) is an exciting part of the future of IT. As organisations move increasingly into this space there is a need for them to review their associated processes, both manual and automated. This is necessary so that businesses can remain in step with, and have confidence in, this new electronic age.

This document is not a code of practice leading to the legal acceptability of electronic documents. Rather, it attempts to provide the reader with an indication of the types of areas that need to be considered.

Introduction

The need for admissibility

When discussing the legal admissibility of electronic documents it is as well to remember that approaching 99.999% of business transactions are completed without incident. Only rarely is there a need to question the business process or associated transaction documentation in a legal context. The problem is that it is not possible to predict which transactions are the ones that will fall into that rogue 0.001%, to which such terms as 'admissibility' and 'chain of evidence' need to apply. So process and associated transaction documentation needs to be acceptable.

If, as part of a case, an electronic document is challenged in Court, the computer systems used for the document creation, dissemination and storage may be called into question. A seemingly acceptable document may be discredited by demonstration that the information has not been created or stored in a proper manner, or that the system is unreliable and not maintained satisfactorily.

An **Information Management Policy**, if properly implemented, can help avoid such challenges by showing that computers and the systems that run on them are a *well-managed* and *clearly documented* part of an *organisation's operation*¹.

An Information Management Policy

An information management policy should address the following issues:

- **Responsibility**, who has the overall responsibility for information management?
- **Access and Distribution**, who requires access as part of a business process and to what specific subset of information is access required? How is such access controlled? How is document² issue and document distribution managed?
- **Retention and Archiving**, which documents need to be retained and how long do they need to be kept?

When documents are no longer required how are they disposed of and who disposes of them?

- **Auditing and system Review**, how often is the system reviewed, what formal audits are required and who carries out these reviews & audits?

The implementation of an *Information Management Policy* requires that there be supporting documentation, operational and training procedures and an associated auditing and assessment regime.

Finally, an Information Management Policy should lead seamlessly into the principles governing the storage of electronic documents within the enterprise's Document and Content Management (D&CM) system.

Principles for a D&CM system

There are five principles that are critical to the effective management of documents held electronically, that is digitally, they cover the following:

- Representation of Information
- Duty of Care
- Business Procedures and Processes
- Enabling Technologies
- Audit Trails

The guidelines in this document cover all types of digital data. A data file may contain text, images, CAD diagrams, moving and still video images and audio or any combination of these data types.

The remainder of this document expands upon the characteristics of a system that will satisfy the Courts that the principles in the above areas are not compromised.

¹ In some instances Courts have requested sight of an 'Executive Authorised' document, which states that electronic documents are used in the normal course of doing business.

² The term document here and throughout this paper implies electronic document. This covers such diverse electronic objects as AVI files, JPEG digital camera images, scanned in paper images and CCTV streams.

Required System Characteristics

Overview

To ensure the authenticity and legal acceptance of information in a D&CM system, it is necessary that the system exhibit certain characteristics. These are expanded upon below but in essence relate to the need to have a system, which is:

- Endorsed by the organisation's management
- Understood by the employees
- Integral to the daily operational processes, both manual and IT supported
- Capable of being audited to demonstrate adherence
- Complete in that maintenance and archiving are included as well as normal operational processes.

Authenticity

The rules of evidence applying to electronic documents are essentially concerned with authenticity and reliability. Particular attention is paid to the sources of information, and the method and time of preparation. With the safeguards that can be built into IT systems, the best evidence is not dependent on the specific technology used to create an electronic document. Rather, it depends on showing that the information recorded was the result of a process or system that accurately produced it. In establishing the authenticity of information, managers may be required to demonstrate in Court or to administrative authorities the trustworthiness of the system used to produce it. They may be required to testify about the operation of the system. In some cases, the opposing parties or the Court may inspect the system.

For specific electronic documents the focus is on the reliability and accuracy of the systems and processes and not on any innate characteristic of the storage format or medium. These attributes are established by:

- The policies and procedures defining proper development, maintenance, and use of the system;
- Ongoing training and support programs that ensure staff understand the policies and procedures; and
- Controls that monitor the accuracy and authenticity of data, the reliability of hardware and software and the integrity and security of the system.

Systems that produce records must be shown to do so in the normal course of business and in an accurate and timely manner. Policies, procedures, training and support programs and controls must be documented to demonstrate that the systems, which produce records, are reliable. Documentation must be understandable, accurate, and accessible.

The stringency of controls incorporated into a system should be commensurate with the degree of risk and the benefits to be gained from effective systems management. The first emphasis should be on business-critical systems, systems that produce records needed in legal proceedings and systems that expose the organisation to a high degree of risk. Systems that use newer technologies, such as electronic filing, electronic document interchange (EDI), digital imaging, and electronic mail, warrant careful review because practices for effective management of new technologies are still evolving. Courts will scrutinise untested technologies more rigorously than established ones, especially where there is no legal precedent.

General Characteristics of a System or Process

The legal acceptance of an electronic document might be challenged on the basis that the process or system is unreliable and hence incapable of producing trustworthy records. The admissibility of information will be less readily challenged on this basis if an organisation can demonstrate that the system that produced it:

- Operated to support a business function and produced any electronic documents as part of that function;
- Created and maintained accurate records; and
- Produced documents in a timely manner, or that the time lapse between an event and the creation of an electronic document had no effect on its content.

Program managers, information managers, administrative support staff, and data processing professionals can take the following measures to ensure that records produced by automated information systems are accurate and timely.

Closeness to the business process

Businesses depend on accurate record-keeping functioning effectively. In both the government and private sectors records are considered trustworthy if they are created in the normal course of business. Information captured to support typical business activities, such as that produced in the regular course of operations, is considered to be inherently more reliable than that produced for litigation³.

Therefore, an electronic document should be created and kept as a part of the regular course of business. The regular course of business is nothing more than doing business in accordance with one's usual habit or custom. The document should also be managed at or *near to the time* of the transaction being undertaken. This management of the document should be by a person within the business with *knowledge* of the associated business transaction.

Creating documents in the course of business is not limited to a pattern of activity that produces documents on a daily, weekly, monthly, yearly, or other cyclical schedule. Many organisations create documents as part of regular programs, but at irregular times. As an example internal audit reports may be produced intermittently as normal activities.

Management should pay particular attention to changes in the cycles or patterns of document creation that may occur when new technologies are employed or when the administration of information systems is decentralised.

Fitness for purpose of the IT system

This requirement is effectively to use best practice and the most appropriate equipment and processes available in the market at the time⁴. Associated with this is the need to ensure the competency of any IT operators.

Written Policies and Procedures

The trustworthiness of information may be judged by the adequacy of existing procedures and how closely they are followed. Policies and procedures should define normal operations for development, maintenance, and use of information systems.

Documented policies and procedures for each system should:

- Describe the methods used to create, modify, duplicate, archive and destroy electronic documents;
- Define the roles and responsibilities of individuals involved;
- Provide training and support to help ensure that policies and procedures are understood and implemented;

³ For this reason business records made for the purpose of legal proceedings are not always accepted.

⁴ So it would not be acceptable, post 2000, to hold a company's business records on a Commodore 64 games computer of 1980's vintage.

- Provide for consistent quality control⁵ and for resolution of problems that may cause inconsistent action or misinterpretation;
- Develop and implement system audit trails to detect who had access to the system, whether staff followed certain procedures, or whether fraud or unauthorised acts occurred or might be suspected in the system;
- Conduct routine tests of system performance to verify the integrity of the system under extreme loads;
- Demonstrate the purpose and uses of the system; and
- Be kept up-to-date and readily available.

Established procedures only show what an organisation *intended to do* in managing and controlling its processes and systems. The trustworthiness of the associated electronic documents depends on how closely procedures are followed. Courts may scrutinise deviations from established procedures, especially if deviations are from legally required procedures. Therefore, additional measures are necessary to ensure that procedures are followed and deviations are detected, documented and remedied.

Training and Support

Formal training and support programs help ensure that policies and procedures are understood and implemented by staff. Instructions for data input, processing, and retrieval should be provided to support training. User access to the system should be granted on 'proof of competence' after training.

Documentation showing that an organisation provided sufficient supervision to oversee staff in the proper use and maintenance of a system will also strengthen the case that procedures were followed. Operation logs and help desk (trouble) reports can document that problems were quickly identified, attended to, and resolved. If an organisation can demonstrate that staff knew what procedures to follow and were overseen and supported by responsible staff, it can also show a Court or other outside parties that procedures were most likely followed⁶.

Retention of Electronic Documents

When retaining an electronic document, certain criteria must be met to make that retention acceptable. The document needs to be retained in the format in which it was made, sent or received or in a format which does not change the information contained within it. Also the information must be readable or perceivable by any authorised individual.

The document should not be retained beyond the duration of the business transaction associated with it except where the retention is to satisfy a legal requirement for the auditing of transactions overall⁷. Finally, the storage of the document must include any information that identifies the origin and destination of the document and the date, time and when it was sent or received.

Retaining documents electronically introduces the additional factor of being able to migrate and read them at a later date. Program version changes may make a document unreadable, or the storage medium may become obsolete⁸. Procedures should be defined for reviewing and updating stored material so that it continues to be accessible.

⁵ Including the selection and storage of a sample set of original documents to provide a known benchmark standard. Use of standard imaging hardware is recommended.

⁶ It is advisable to keep records of attendance at training sessions and certification of training. It is advisable to implement a test as part of the training in order that an individual's competence can be proved later.

⁷ A separate section of this paper references an archiving policy. The archiving of electronic documents needs to be directly related to the legislative framework that applies. For example it may be necessary to keep the documentation associated with aspects of Health & Safety at Work for a different period of time than those associated with financial accounting requirements.

⁸ Current computers do not support for example 5¹/₄" floppy disks, common less than a decade ago. Many new machines are sold which have a CD drive but no floppy disk drive.

Migration

For some technologies it may periodically be necessary to convert, regenerate, copy, or transfer information from one medium or technology to another to preserve the information for the full retention period. The need is to be sure of reliable access to information stored over a period of perhaps twenty or thirty years which may be beyond the design and operational life of both drives and media.

With fast moving technology long-term storage⁹ has not been tested in real life. Regardless of the established retention period or the life expectancy of the media electronic records must continue to be maintained when litigation, government investigation or audit is pending.

Web Sites

As electronic trade has become more widely accepted web sites have been constructed which offer a 'dynamic and changing' shop front to the end consumer. On such sites the web page 'viewed' by the user may not actually exist, but may be constructed 'on the fly' using a combination of such technologies as *content management* and *active server pages*. This creates a dilemma with regard to the storage of a specific web page for future legal reasons. In such situations, it is necessary to hold sufficient information to enable the web site to be 'recreated' as it existed at a point in time for that user. A log of changes to the underlying database, which feeds the web site, along with an audited record of changes to the software and other details regarding the operation of the web site needs to be held.

Destruction

A system can become inefficient or unusable if material that is no longer required is still retained. Part of any retention policy is the weeding, and either archiving or destruction, of material no longer required. The identification and deletion of unnecessary files should be as regular and systematic as the identification of material to be retained.

Errors

Correcting information in an electronic document involves maintaining the original, incorrect entry and adding a correction. The original document content should not be altered or obscured in any way. The reason for the change should be indicated as well as the date and time and the name and authority of the person making the amendment. In D&CM terms this means that a system will hold both the original (frozen) and the amended copy.

The original, unaltered document must remain as part of the D&CM system and must permit access to the original document on demand. This access is especially true for external auditors. The original document should reference the new document via some tagging which relates the original to the amended document¹⁰.

System Controls

Effective D&CM systems need mechanisms and controls to ensure the quality and reliability of the information they contain. These controls will monitor input and output processes, hardware and software performance, and security. They should be an integral part of the system, built into it during development, embedded in operating policies and procedures, and implemented through ongoing training and support.

⁹ For example it is essential to document the program, algorithm and version of any compression mechanisms used for storing files.

¹⁰ A D&CM system will normally implement a freeze, checkout, amend, check in and associated version control system for documents.

Audits

The purpose of an audit is to confirm that a system or process produces accurate results. Independent persons, such as internal audit staff or outside independent auditing firms, conduct audits. Independent implies having no contact with the creation process for electronic documents and having no interest in the content of such documents.

With the increasing complexity of most operations and the introduction of new technologies, the accuracy of information systems is an audit concern. Many audits address financial and program issues rather than the accuracy of information systems. Almost all audits use records that originate from information systems.

Because auditors must concern themselves with the relevance, validity, and sufficiency of evidentiary matters, the accuracy of records and the reliability of the systems that produced them come into question during the course of most audits. Managers are responsible for complying with any program, financial, or performance audit requirements that rely on creation and maintenance of accurate and trustworthy records.

Audit Trails

An audit trail is used to determine the path of a document through the system. The general points on audit trails are easily maintained by D&CM systems utilising structured workflow, but are not so easy to maintain with systems using ad hoc workflow documents where the trail of a document is not recorded.

There should be little trouble with optical storage requirements, but batch data audit trails can potentially be a problem. For example, a day's scanning may be referred to as a batch in paper terms, but may result in additional, unwanted documents, in the associated files on a D&CM system. Where a batch of documents is large it may not be easy to subdivide it and/or retrieve individual documents later. Where a batch of documents

is small there may be too much of an operational overhead in the capture and control process. The balance between the two has to be resolved at an individual organisation level.

System Audit Trails

A system audit trail will document who used the system, when they used it, what they did, and what the results were. Effective audit trails can automatically detect who had access to the system, whether staff followed certain procedures or whether fraud or unauthorised acts occurred or might be suspected in the system.

Properly implemented audit trails¹¹ track:

- Changes to data in a system, including the creation, modification, and deletion¹² of records;
- The date and time of changes; and
- The source of changes.

Testing System Performance

With the increasing amount of business transacted electronically it is important to test system performance regularly to verify the integrity of a system *under conditions of extreme load*. The design and use of system and performance harnesses and tests should be documented, because the reliability of information contained in the system will depend on the accuracy and reliability of the programs and procedures used to create, modify, and retrieve them.

¹¹ System audit trail mechanisms are subject to strict procedures to ensure their validity.

¹² Some systems do not allow a user to delete documents. In which case they are tagged as being logically deleted and then archived such that an audit trail is kept of deleted documents. Having been tagged as deleted they are not then visible to the user.

Hardware and Software Reliability

The reliability of hardware and software affects the authenticity and admissibility of documents. Equipment, which is not functioning properly, can alter the content of computer records; the reliability of the IT equipment used to store and produce information may be challenged. Errors in electronic records can also result from errors in the computer programs used to create those records.

Organisations can enhance the acceptance of computer-generated information, if they:

- Routinely test hardware and software according to a plan developed in consultation with the manufacturer;
- Retain all documentation related to hardware and software procurement, installation, and maintenance; and
- Maintain operation logs and run schedules to document the reliability of system operation and performance.

System documentation demonstrating compliance with the manufacturer's hardware maintenance requirements, evidence of the development and testing of programs, and a history of consistent use and reliability of hardware and software, is normally sufficient to demonstrate the reliability of systems. An organisation may also be required to facilitate access to individuals who can testify about testing and dependability of hardware and software.

Security

Secure IT systems furnish an ideal environment for creating and maintaining trustworthy information. To provide for security, system developers need to develop routines that limit access and update privileges to the appropriate people and prevent unauthorised access to and modification of data. Such provisions must be documented so they can be used when attesting to the credibility and trustworthiness of the system. If the security of an organisation's computer system can be called into question, the validity of a piece of evidence drawn from that system can also be challenged.

Physical security is often overlooked when considering electronic document systems because of the emphasis on technology. However, integrity and authenticity of documents produced or stored by an organisation can be easily jeopardised or called into question by a lack of physical security in an organisation.

If unauthorised personnel have access to the premises, it is possible that they could also gain access to computers. If terminals/PCs are left logged in but unattended, files could be altered or material sent from another user's address. If possible, file servers and associated optical storage should be contained within a secure area¹³. This area should be accessible to authorised personnel only.

Likewise, if an organisation has not installed a suitable electronic security system¹⁴, outsiders may hack into the computers and modify files or make use of the address to send files. Such breaches of security are by no means common, and require considerable effort on the part of the person acting in a criminal manner; however, the potential for such attack could be used to discredit electronic evidence.

Recovery from Failure

Disaster preparedness plans and security backup procedures, which are proven *operationally* on a regular basis, will ensure that electronic documents are protected against inadvertent or accidental loss or destruction. Similarly there is a need to document any use of backup procedures to restore a system or recover documents, especially if backup procedures were used to regenerate a document.

¹³ This is not always possible as document management systems are often sold as departmental solutions and as such are installed locally to that department.

¹⁴ Including an appropriate mechanism for guarding against the introduction of viruses from both internal and external sources.

Role Separation

Organisations can enhance security by dividing the duties of staff such that individuals with an interest in the contents of electronic documents are not also responsible for administering system security, quality control, audit, or other tasks. This reduces the chance of the integrity of a system being compromised or called into question.

In extreme situations an additional level of role separation may need to be introduced, for confidential and secret correspondence, to ensure that friendships and family groupings do not compromise security.

Accuracy and Timeliness

The processes used for data input and output must produce accurate and timely records. Input can be challenged on any of the following grounds:

- The manner in which documents were entered into the system initially;
- Whether the documents were entered in the regular course of operations;
- Whether documents were entered within a reasonable time after the events recorded; or
- The adequacy of measures taken to ensure accuracy of the documents.

Adopting the following measures enhances the acceptance of documents generated through processes that involve input and output:

- Develop and follow systematic procedures for data entry;
- Design, implement, and document quality control procedures including preparing documents for scanning and checking them for suitability¹⁵;
- Identify all input and output documents and procedures in the system documentation;
- Confirm the accuracy and validity of records at the time they are created or updated as part of the process;

- Document any delays in data entry by noting the date the source documents were created and the date the data was entered, and keep records of any unusual delays in producing output;
- Retain any specially written program used to extract data from a system; and
- Produce labels for media containing electronic records that identify the exact title (including the name of the system), creating unit, date, purpose, source, and destination of the records.

The Scanning Process

In many user manuals, the process of scanning is described just as “Scan”. In general operation, more detail is required.

For example, the system should give each document a unique identity number, which cannot be altered. Most systems are able to perform this function. The date and time of scanning and the identity of the scanner operator should be logged. Also a log of post-scanning activity performed on the document should be maintained. For ad hoc workgroup applications this can be difficult. Processing detail is often only kept if structured workflow is used.

Information should be stored about scanned batches of documents and the activity carried out in those batches. Where document batches do not match a pre-defined workflow, this can be difficult. It can create a huge overhead and may be impractical. The task may be carried as part of manual working practice rather than as part of the D&CM system. Where an automated document feeder is used, special care should be taken to ensure that all documents are properly scanned. This is usually done intuitively by the scanning operators and may be difficult to prove.

¹⁵ For example staff may intuitively remove staples or photocopy documents, which are known from experience not to scan well. This should actually be a documented procedure, which indicates, for example, the conditions under which the documents are re-stapled.

Indexing

Indexing should be detailed in the user manual. Indexes need to be backed up and secure as images are of little use if they cannot be retrieved. It is good practice for a copy of the relevant part of the index file to be kept on the same optical disk or magnetic volume as the document to which it relates. This can create a difficulty as few optical systems write the whole index to the optical disk or leave space on optical disks for changes. This is more usually done on a magnetic medium. Requirements in this area may necessitate changes to the way optical storage systems work.

Information about the date and time of creation and amendment to index data should be recorded in the audit trail, along with the actual change itself. The overhead of keeping this detail on indexes can be huge and may have a high development cost associated with it. This information may not be of use to the actual business process therefore the impact and risk of not keeping it may need to be assessed.

System Documentation

Complete and accurate documentation of the system or process that produced or captured electronic documents is essential to demonstrate that information is trustworthy. Documentation provides verification of the processes used to capture and store electronic documents. Proper documentation preserves information, independent of the individuals involved, on all aspects of system design, implementation, maintenance, and oversight. It demonstrates the existence and proper operation of system controls, which ensure that records are accurate, reliable, and authentic.

During the design of the system a knowledgeable person should prepare and maintain documentation for the process or system used to capture and contain electronic documents. Documentation should be complete and up-to-date, and documentation of all changes to a system must be kept for the full retention period of any records produced by the system.

The following guidelines will help organisations to produce and maintain quality documentation that supports the admissibility of records:

- Documentation should be comprehensive, covering all components of an information system, and demonstrating all steps from the beginning to the end of the process;
- Documentation must be accurate and be prepared and maintained by knowledgeable staff;
- Operational documentation should be written aimed at the appropriate training level and technical competence of the operators; and
- Documentation should be current and immediately available if needed for Court proceedings or other purposes.

Courts may require documentation that shows how the system operates; training documentation to show the distribution of written instructions, the nature of course materials, the attendance of individuals at training or refresher programs and certification for completed training and audit trail records to show what activities occurred in the system and provide evidence that procedures were followed. Also, individuals familiar with the operation of the system may be asked to testify.

Retention of Documentation

Sufficient documentation should be retained for at least as long as any records produced by a system are retained. It should describe how a system operated and delineate the meaning, purpose, structure, logical relationships, and origins of data. When a system is modified or replaced, older versions of the documentation should be kept for as long as any records created by that version of the system. Procedures used for migration or conversion of records to a new system should be fully documented. Destruction, deletion, or other disposal of documentation must be conducted in accordance with agreed retention and disposal policies and schedules.

New Technologies

Courts readily accept records produced by legacy information processing methods and technologies, such as writing, typing, photocopying and microfilming. Many of the policies and guidelines that permit use of reproductions of electronic records are based on decades of experience with micrographics technologies and established standards for quality reproduction using microfilm.

Records produced or reproduced using newer technologies, such as digital imaging and electronic document interchange (EDI), are generally subject to greater scrutiny until their reliability is established through experience and widespread use. In the absence of proof to the contrary, there is a presumption that any device used in the preparation or reproduction of the document is reliable and accurate.

Organisations should take special precautions when introducing new technologies that will enhance the reliability of their record keeping systems and increase the likelihood that records produced by such systems will be legally acceptable.

Originals Versus Duplicates

The traditional bias in the 'rules of evidence' in favour of original documents over duplicates has largely been overcome by legislative reform. Emphasis has moved towards ensuring that *proper procedures* are followed and safeguards are in place to produce reliable and trustworthy records. In the context of Court proceedings, an "original" of a record is the record itself. In the case of electronic records, a strict interpretation of the term "original" is impractical because a computer record cannot be viewed or read unless it is printed or displayed in a "human-readable" form.

To deal with this problem of 'reading' electronic originals, legislation has been widely¹⁶ enacted which permits the admission of computer printouts and other eye-readable¹⁷ renderings of computer records, provided that they accurately reflect the information in the original

recording. In addition, Courts have been willing to treat computer printouts as a form of real evidence, not subject to the rule against hearsay or the best evidence rule, provided that the accuracy of the printout was not affected by human intervention and provided that the machine was operating reliably.

In the case of records that are reproduced by scanning and storing them as digital images, the digital image or a printout of the image may serve as the best evidence, in lieu of the original, if satisfactorily identified and reproduced by an *accurate process* and medium. When scanning a photocopy of an original this should be recorded by, for example, an index reference¹⁸.

Duplicates of electronic records must accurately reproduce the original records. Information that is readable or recognisable on originals should be readable and recognisable on duplicates.

If image enhancement techniques are used, the information that is readable or recognisable on duplicates must also be readable or recognisable on originals, except that duplicates may also contain production, control, indexing, certification, or other data not related to the informational content of the records. This exception allows additional data to be included on duplicates for administration of the reproduction process if it does not adversely affect the informational content of the record. Control and indexing data stored with digital images, for example, may be necessary to retrieve the images, but must not affect the content of the records themselves.

¹⁶ Geographically - and under different legislative regimes.

¹⁷ An AVI or multimedia file may include sound playback synchronised with a visual image.

¹⁸ For back file conversion of existing files, any photocopy in the file such as the photocopy of a birth certificate should be identified as a photocopy on the electronic copy because this will not be obvious when subsequently viewed. This overhead should be borne in mind when deciding upon back file conversion.

Digital Imaging

Digital imaging uses scanning technology to convert documents to an electronic form. Each page of a document is converted to a digital image. This image can be thought of as equivalent to an electronic photograph; it is an exact replica of the page (within the physical limits of the scanning process). Images are stored on magnetic or optical media from which they are retrieved and displayed on computer screens or reproduced on paper.

Without further processing it is only possible to 'view' the image on screen or print it. The system "knows" nothing about the content of each page; it would not be possible to search¹⁹ for a document containing certain text, or import the text of the scanned document into a word-processor.

Special precautions must be taken to ensure legal acceptance of digitally produced images because imaging is a technology with the potential for image enhancement and alteration. In secure systems, printing (and copy, cut and paste) are disabled such that the user *can only view* the image.

For digital images to be useful, it is necessary to have some way of finding the images relating to a document of interest. One or more index fields are normally captured for each document scanned. These index fields are stored on a 'file card' associated with the image. This file card is referred to as 'Meta Data'.

Organisations using digital imaging technology should implement the following measures as part of the normal operation of an imaging system:

- Verify that the system accurately reproduces all originals so that any information, which is readable and recognisable in the original, can be recognised on the digital image²⁰. Visual verification of each image may be necessary if automated verification is not provided by the system. The methods and criteria used for image verification should be described in the documentation of the system's operating procedures.

- To ensure long-term availability of the image in its original form compress the image using standard compression and decompression algorithms²¹. Proprietary algorithms do not guarantee the same degree of long-term readability and trustworthiness.
- Image enhancement may be used to increase the legibility of documents in imaging applications. Nevertheless, use of ITU compression standards to preserve a record in its "originally captured form" is recommended. Any use of image enhancement must be part of normal operating procedures that are thoroughly described in the system's documentation.
- Institute special security provisions to prevent alteration of digital images. System security features, such as password-controlled access and update privileges, operation logs, and audit trails deter alterations and enable detection of unauthorised modifications to records. See also Security and Role Separation.
- Use Write-Once-Read-Many (WORM)²² optical media for imaging applications.

¹⁹ A separate process of Optical or Intelligent Character Recognition, O/ICR, may analyse the 'photograph' and attempt to recognise and reproduce the text on it. This reproduced text will be held in a separate associated document and not in the original digital image. Such techniques can be used to assist in locating certain text.

²⁰ Some imaging applications include utilities that automatically verify the accuracy of the image when it is written.

²¹ Such as those established by the International Telecommunications Union (ITU).

²² WORM media cannot be modified after the initial recording. It combines the unalterable qualities of microfilm, with the speed and accessibility of electronic records.

Electronic Data Interchange (EDI)

Electronic data interchange (EDI) is the computer-to-computer exchange of business data in a standard format²³. Most EDI applications include special measures to ensure authenticity as a substitute for the signatures on paper documents that have been used traditionally to authorise business transactions.

For EDI to work as an effective and reliable method of transacting business, the trading partners involved must reach agreement on a number of technical and use standards relating to data exchange. Technical issues include provisions for the structure and format of data into transactions sets (also called “documents”), the transmission of formatted data, the standards for communications, and security procedures.

Issues related to contract formation, validity, and enforceability have to be addressed specifically within the context of each EDI relationship (e.g. the time and manner in which electronically transmitted messages become effective, what constitutes an electronic “signature,” and the proper course of action in the event of an unintelligible transmission need to be established in contracts or memoranda of understanding among the trading partners).

Records Management

Records Management is a separate discipline that deals with records of all types, in all formats and on any media, it requires that records be retained and maintained until a ‘disposal authority’ is approved. Disposal authorities are usually in the form of disposal schedules, which state minimum retention requirements and provide a systematic process for the disposal of records generated or acquired²⁴. The schedules are developed co-operatively and take into account the continuing value of the records to Government and the community.

A range of criteria are used to determine the length of time for which records should be retained, these include legal accountability as well as administrative, research and historical documentation requirements.

A number of additional issues need to be considered when determining whether to authorise the destruction of source documents that are stored electronically or records that have been converted to digital images. In order for electronic records to be accessible they must remain readable and intelligible. In an era of rapidly changing technology that utilises proprietary systems and methods, long-term access to electronic records may be difficult to ensure. Factors such as the length of the retention period, hardware and software obsolescence, media longevity, vendor stability and conformance with widely accepted standards must be considered when determining whether retention of electronic or digital images is sufficient to satisfy minimum retention requirements or whether a paper or microform backup should also be retained.

In the UK the Public Records Office sets standards in the area of Records Management.

For more information in this area see www.pro.gov.uk/recordsmanagement/

Periodic Assessment

On a regular basis the ‘contents’²⁵ of a D&CM system should be assessed and evaluated. This periodic assessment and evaluation of systems provides evidence that procedures are being followed and support the system and process documentation.

²³ Increasingly this makes use of XML, eXtensible Mark-up Language.

²⁴ Usually relating to information retained by Government agencies.

²⁵ This does not mean that every individual item is viewed, rather that a check of where, why and how information is kept.

Admissibility and Rules of Evidence

Common Law Rules

Evidence, which a Court will accept, is known as “admissible evidence”. Documentary evidence can take a number of different forms. In essence, so far as the law of evidence is concerned, the concept of a document involves:

- Some physical thing or *medium*
- On or in which *data* is
- More or less permanently recorded
- In such a manner that data can *subsequently be retrieved* (with the proper equipment).

Modern rules of evidence address two principal common law exclusionary rules applying to documentary evidence - the best evidence and hearsay rules.

The **best evidence rule** precludes the admission of any documents other than the original, barring an acceptable reason for the absence of the original.

The rule against **hearsay** prohibits use of a document as proof of the facts contained within it. For example, a letter which states that a person was in London on a particular date could not be admitted to prove that the person was, in fact, in London on that date.

Strict application of this type of rule can result in the exclusion of evidence that is cogent and reliable. Therefore, various legislatures have created exceptions to these exclusionary rules. Increasingly, these make provision for the admission of both electronic records and documents in traditional formats.

Exceptions to Common Law Exclusions

A document must satisfy precise legal requirements before it will be admissible under an exception to the hearsay or best evidence rules. The rules of evidence referred to below appear to be generally applicable in both civil and criminal proceedings in most jurisdictions. The rules are more stringently applied in criminal proceedings, where documentary evidence is subject to greater judicial scrutiny, to ensure its reliability than may be the case in civil proceedings.

Generally, it is easier to ‘prove’ the authenticity of public documents, official and business records, and documents and evidence produced by clearly documented and understood business processes.

Legislation achieves this by:

- Creating presumptions concerning the accuracy and reliability of the processes that produced the document;
- Creating presumptions as to the authenticity of seals and signatures;
- Enabling evidence of official records to be adduced²⁶ by the production of the record or a copy of it; and
- Creating a presumption in favour of the accuracy and authenticity of official records and extracts, copies and summaries of public documents.

Presumptions may be challenged if evidence is adduced raising a doubt about their application in a particular case. Accordingly, in spite of the flexibility and simplification injected by various laws, it remains important to ensure the accuracy and reliability of information systems.

²⁶ Cited or used as an instance.

Public Documents

Exceptions to the best evidence and hearsay rules are to be found when dealing with so-called *public documents*. Statements in public documents are generally admissible evidence of the truth of their contents. Public documents²⁷ are those made by a public officer pursuant to a public duty to inquire and to record certain facts for the purpose of the public making use of them and being able to refer to them.

Generally, before a public document can be *received* into evidence it must be shown that the document is *what it purports to be*; that is, it must be properly authenticated. The proper official seal, signature or certificate on a document affixed by an authorised officer is generally sufficient proof of the authenticity of most public documents without further identification. Similarly, proof of designated official and public documents is facilitated by the provision of presumptions as to the validity of those documents and of official seals and signatures.

Commonly legislative schemes provide an exception to the best evidence rule for *copies* of public records by establishing mechanisms by which such copies may become self-authenticating. In order to free custodians of public records from the burden of testifying in Court that copies of records in their possession are genuine copies, the legislation provides that where documents are able to be proved by a certified copy, the *production* of such copy will suffice. It is not necessary to prove that the copy was examined or certified by the person whose seal or signature is affixed to it and no proof of the authenticity of the seal or signature is required. In addition, whenever the original of a public document is admissible at common law, these statutory provisions enable a copy to be adduced if it purports to be signed and certified as a true copy by the authorised custodian. It is not necessary to prove that the copy was examined against the original.

Evidence for Administrative Hearings and Regulatory Proceedings

Administrative tribunals and regulatory authorities generally have different rules from Courts. Generally, tribunals and authorities of this nature are established by statute. The relevant establishing statute often makes provision for the rules and procedures to be applied by the body in conducting hearings. Commonly, this provision is to the effect that the rules of evidence do not apply or are not to be strictly applied. Alternatively, the statute may empower the body to make its own rules with respect to evidence and procedure. In the absence of such legislative direction it is open to debate whether all or any of the rules of evidence apply to the proceedings of such bodies. Where the rules of evidence do not apply, the tribunal or regulatory body has greater discretion than Courts in determining what evidence will or will not be accepted in its proceedings. Even where the formal rules of evidence do apply to such a body, a more tolerant and flexible attitude to those rules is likely to be taken.

Regardless of whether the rules of evidence apply or apply only in a modified form, records submitted at a hearing must still be shown to be accurate and reliable.

²⁷ Birth and marriage certificate are common examples.

Jurisdiction

Decisions about the creation, maintenance and use of documents and their management systems must be made in the context of laws and rules of general application as well as legislation (if any) under which an organisation operates. The management of information must comply with applicable laws, regulations and agreements, with established professional practices and standards, and with applicable administrative rules and policies.

When operating in the UK for example, the data concerned may have originated from outside the UK or have been transmitted over communication lines, in which case the “best practice” procedures will apply.

Legal Systems

The term ‘legal’ implies subject to a legal system. In the world (and in terms of legal admissibility we are often talking about international trade) there are different styles of legal systems. In each of these different systems there is the possibility that the burden of proof may be different. In all of them the essence is to demonstrate that proper processes exist and were adhered to.

Duty of Care

The final point is that when implementing a D&CM system it is advisable that consultation takes place with commercial departments, internal solicitors, internal and external auditors, the company secretary and relevant regulatory bodies. Until recently, there is likely to have been a widespread lack of knowledge about this subject, therefore these groups of people may need to understand the issues around a D&CM system and become familiar with the issues. It is a good idea to give a project member actual responsibility for the required consultation work and to monitor feedback and manage any objections.

Sources & Acknowledgements

Acknowledgements

In writing this paper references have been made to the contents of a variety of web sites and associated publications, too many to mention here.

The wording and process breakdown on many of the web sites is similar. This suggests that there is a source document somewhere from which many of the web site words have been cloned. This may well be *Guidelines for the Legal Acceptance of Public Records in an Emerging Electronic Environment*, published by The State Archives and Records Administration, New York State, 1994. It may alternatively have originated from a South Australian web site, as they were leaders in this area.

Examples have been extracted from State and Government web sites such as those for the Australian state of Tasmania, the US state of Alabama and the Canadian state of Ontario. Information from these sources has been supplemented and crosschecked with 'Standards Agency' web sites such as those for the BSI, ISO and CGSB.

For more details on security, reference can be made to the British Standard BS7799 - *A Code of Practice for Information Security Management*.

A code of practice from the British Standards Institute (PD0008²⁸) provides a framework, which will help users maximise the value and integrity of that data, which may have to be produced in a Court of Law as evidence. It is likely that Judges will look to this document as a benchmark for their decisions.

²⁸ A Code of Practice for Legal Admissibility and Evidential Weight of Information Stored Electronically.

FUJITSU SERVICES

Observatory House, Windsor Road, Slough, Berks SL1 2EY

Telephone: +44 (0) 870 242 7998 Facsimile: +44 (0) 870 242 4445

E-mail: askfujitsu@services.fujitsu.com Web: services.fujitsu.com

Fujitsu Services endeavours to ensure that the information in this document is correct and fairly stated, but does not accept liability for any errors or omissions.
© Copyright Fujitsu Services Limited 2002 Printed in England 05/02 Ref: 1033