Whitepaper

Electronic document admissibility and retention

Mark Palmer, Director of Product Management & Marketing, Invu

Electronic document admissibility & retention

Volumes of company information, paper files, electronic documents and emails continue to accelerate. Legal requirements and good practice from regulatory bodies demand the retention of considerable amounts of documentation for many years before destruction. For physical documentation, this may be impractical or at least costly, slow and inefficient. Worse still, is the scenario where misfiling means employees spending hours hunting documentation, sometimes under deadline pressure.

Technology has tilted the balance from the physical paper document towards more electronic transactions and documentation. Capture technologies and electronic document management systems (eDMS) have revolutionised the processing and retrieval of paper documents. By bringing them into the electronic world with the rest of the documentation (be it MS Office documents, emails, line of business documents) there are clear and proven benefits:

- Enhanced effectiveness and efficiency gains
- Superior information sharing/ knowledge management, specifically limiting information silos, particularly email
- Improved customer/client/supplier service levels

Reluctance to change – is it safe to destroy originals?

There are undoubted advantages in adopting eDM but also perceived barriers to change. Paper documents and files are extremely vulnerable to loss and destruction but they are tangible and, if untampered, give absolute proof. This understandable comfort blanket effect will stop many businesses from grasping the eDM nettle or at least doing so whole-heartedly. “Destroying the physical evidence” feels unnatural so it’s important to know that the eDM you choose is not only a good software choice, but that the ensuing improvements to operational process will not put your organisation at risk.

The need to preserve original paper documents once scanned and captured is the most common query faced by eDM/ ECM providers. Most organisations will want to destroy original paper documents, free up filing space and stop using physical storage with all the inefficiencies entailed.

In the vast majority of cases original documents do not need to be retained. However, certain key documents will need to be retained – most notably artefacts proving tax deducted for HMRC purposes and signed leases, title deeds and contracts. The most sensible policy to adopt here is to retain what is obviously most legally critical and, if you are unsure then seek further advice from any relevant professional body (ICAEW, HMRC, Law Society etc.)

Most operational documents can be destroyed without fear of comeback. After all, once captured electronically and saved, the document is available more quickly and with more accuracy than any physical filing system. Once lodged in the eDM/ECM system the document will always be retrievable.

However, where an original document is destroyed and there is a subsequent dispute which ultimately could go to Court, how credible is your scanned and saved copy? Can it be used to produce reliable evidence to defend any case?

Meeting a Court’s requirements for highly reliable evidence is where the issue of “Legal Admissibility” comes into play

Natively electronic documents vs. scanned documents

The term electronic documents covers Word documents, Excel spreadsheets, emails etc. Like paper-based documents, if the provenance of a document is clear and its integrity is incontestable then admissibility is not considered an issue. Courts and governing bodies now recognize day-to-day working practices and accept electronic documents as evidence or supporting material so long as companies can prove that they've taken the appropriate measures to ensure their integrity. Paper documents will be similarly measured but the transition from the physical to digital must be an honest, untampered transformation; a genuine image which cannot be altered and cannot be repudiated. This is at the heart of any reluctance to move to a document management system – can this transformation be trusted? For this, we must consider not only the eDM technology but also the business processes at work.

Legal admissibility

There are two main cornerstones to legal admissibility of electronic documentation:

- The Civil Evidence Act 1995
- The British Standards Institute's BS 10008:2008 (*Evidential weight and legal admissibility of electronic information Specification*). [1]

1995's Civil Evidence Act enshrines the concept that electronic documents carry the same evidential weight as physical signed documents. BS 10008:2008 gives a detailed working practice framework covering both technology requirements and business processes to ensure that an organisation can prove that the content of a particular electronic document or data file has not changed since it was stored in the secure document repository. In doing so the organisation can prove that, it is a true representation of the original. To ensure legal admissibility your documents will need to be retained in a BS 10008:2008 / BIP008 compliant eDM system.

The Civil Evidence Act 1995

This is one of the most important acts in the UK. Here the onus is to move the question of admissibility to actual evidential weight carried by the scanned document. This is determined by the procedures followed by a company presenting any documents to the court.

A company presenting documents that have not been altered since its creation or has a clear audit trail that shows any and all changes since its creation holds a greater 'weight' than a document that cannot show these procedures.

An organisation needs to be able to prove (to a court of law or some other statutory body) that the contents of a particular document or data file created or existing within an Electronic Document Management System

---

[1] BS 10008:2008 encapsulates the prior code of practice (BIP008 *(Code of Practice for Legal Admissibility and Evidential Weight for Information Stored Electronically)*. BIP008 is also known as BSI DISC PD008 and follows a line of evolving guidelines since 1996.

The publication of BS 10008 reflects the demands of the adopters of the Code of Practice (CoP) for a more formal compliance standard and covers the scope of the all three parts of the Code of Practice (BIP 0008-1, BIP 0008-2, BIP 0008-3). The Code will be updated in accordance with BS 10008.

Implementation of the recommendations given in the latest edition of the CoP will assist with compliance of BS 10008.

have not changed since the time of storage. If the data file is an electronically stored image of an original paper document, an organisation must be able to prove that the electronic image is a true representation of the original. Proving the authenticity of electronically stored documents is crucial to their admissibility in a court. In England and Wales, the main statute governing the admissibility of documents is the Civil Evidence Act 1995. This Act resolved many of the outstanding legal difficulties that had arisen through the use of computers for information storage.

The Civil Evidence Act shifted the argument from legal admissibility to evidential weight or value. It makes it easier to prove the authenticity of documents, by producing the original or a copy, irrespective of the number of removes between the original and the copy and irrespective of whether or not the document is a paper one or an electronic one. The court needs to be satisfied as to the authenticity of the copy, and therefore an organisation needs to be able to demonstrate that it has administrative procedures that will satisfy the court as to a document's authenticity.

Sections 8 & 9 of the act demonstrate the legal guidelines for electronic documents as evidence:

1. *Where a statement contained in a document is admissible as evidence in civil proceedings, it may be proved:*
   a) by the production of the original
   b) whether or not that document is still in existence, by the production of a copy of that document or of the material part of it, authenticated in such a manner as the court may approve.
2. *It is immaterial for this purpose how many removes there are between a copy and its original*.

Section 9 states:

1. *A document that is shown to form part of the records of a business or public authority may be received in evidence in civil proceedings without any further proof.*
2. *A document should be taken to form part of the records of a business or public authority if produced to a court a certificate to that effect signed either by an officer of the business or authority to which the records belong. The law can be interpreted to show that an original document is not the only admissible evidence in a civil court. Electronic copies of documents are acceptable so long as their integrity can be shown. The criminal court system which is based upon 'beyond reasonable doubt' involves different requirements and businesses wishing to adhere to these should consult a specialist lawyer.*

The above information will lead to the question of how to show integrity and the level of standard companies are required to adhere to for their document management needs. BS10008:2008 provides guidance here.

More about best practice – BS 10008:2008

BSI 10008: 2008 is based on BIP0008[2]. Also known as ISO 15801:2009, this is the key paper setting a benchmark for procedures that businesses should follow in order to achieve best practice, and therefore, legal admissibility of their electronic documents. It is supplemented by BIP0008 2:2005 *(Code of Practice for legal admissibility and evidential weight of information communicated electronically)* & BIP008 3:2005 (*Code of Practice for legal admissibility and evidential weight of linking electronic identity to documents.)*

To ensure full compliance with the British Standard an organisation requires both certified document management systems and complimentary enforceable working practices.

Compliance with BIP0008 will ensure that the organisation manages its information according to best practice, thereby maximising the chance of electronic records being satisfactorily authenticated.

[2] As an indication of the weight of BS 10008: 2008 and BIP0008, both are referenced in the Freedom of Information Act 2000: Code of Practice on Records Management

It states that an organisation will need to have in place the following five information management components:

1. *Representation of Information (i.e. an information management policy)*
   - *Recognition and understanding all types of information within the organisation*

2. *A Duty of Care*
   - *Understanding all legal issues and execution of appropriate 'duty of care' responsibilities*

3. *Business Procedures and Processes*

4. *Enabling Technologies*
   - *Including document management, content management and records management systems*

5. *Audit Trails*

Importantly, these principles are 'device independent' i.e. that they remain constant irrespective of the technology in use.

The first and last bullets are especially noteworthy – a comprehensive and rigorous policy ensures that there is a clear framework, which the organisation has sponsored; this is policed and validated by audit. (In the same way that the document copy must be authentic and non-repudiable then the associated audit trail must not be alterable.) For BIP008 purposes this gives a mechanism to establish adherence to the policy and also a quality benchmark. The information management policy should be manifest throughout the organisation as a standard operating policy to ensure that it permeates into day-to-day working practices. A good eDM/ECM system will ensure that this policy is followed providing it is not sidestepped by errant staff.

A summary of BIP008 can be found in appendix 1 in this whitepaper.

With BIP008 as the bedrock of good practice, let's look at the advice from some of the key regulatory bodies:

Law Society

The Law Society gives its position in *Guidance – ownership, storage and destruction of documents*. Destruction of originals (notably deeds, guarantees and certificates) is advised only where express permission is received from the owner. The same is true where records are destroyed or expunged. Written evidence of the destruction of originals and identification of any copy is also advised to add weight for evidential purposes. This is in line with good working practices á la BIP008.

HMRC

HMRC guidelines can be found at http://www.hmrc.gov.uk/manuals/chmanual/CH13000.htm. In particular, http://www.hmrc.gov.uk/manuals/chmanual/CH13400.htm echoes BIP0008, stating that "*Where information is preserved on computer media, a copy of any document forming part of the records is admissible in evidence in any proceedings before the tribunal as if it were the original."*

http://www.hmrc.gov.uk/manuals/chmanual/CH13100.htm provides guidance on the destruction of original documents: "*If a person preserves the information contained in paper records on computer by transferring the information into an electronic form, they may discard the paper* ***provided that*** *the method of storage used is capable of*

- *capturing all the information needed to make a correct and complete return, and*
- *reproducing that information in a legible form.*

If the method cannot do these things, the person must also retain the original documentation."

However, some originals do need to be preserved. Tax Bulletin 37 states that "*We accept of course that companies which store information in accordance with the Code of Practice on the Legal Admissibility of Information stored in Electronic Document Management Systems (BSI 1996 DISC PD 0008*) will thereby automatically satisfy the tax requirements.*

The exceptions, where the original record must be retained, are set out in Paragraph 22 of Sch 18 to Finance Act 1998. In essence they consist of vouchers for tax suffered or for tax credits in respect of incomings. But photocopies of foreign tax assessments, rather than the assessments themselves, will remain acceptable for the purposes of claims to double taxation relief in respect of foreign tax underlying "dividend income from abroad."

Specific documents to be preserved are set out in *http://www.hmrc.gov.uk/manuals/chmanual/CH13300.htm*

At present, under the terms of the Companies Act, for most companies the timescales that the Revenue requires material to be retained is set at six years from the end of an accounting period. In cases of investigation or late return submission, then this period will extend accordingly.

Companies House

http://www.companieshouse.gov.uk/about/policyDocuments/legalAdmissCompDoc.shtml sets out Companies House policy: "*If a document is admissible in evidence, then an electronic image of that document may be treated as secondary evidence in the same manner as a photocopy or a microfiche image. It will be subject to the provisions regarding authentication contained in the Civil Evidence Act 1995 in England and Wales and the Civil Evidence Act (Scotland) 1988 in Scotland.*"

FSA

The FSA Handbook is neutral on the subject stating only that "*A record may be in any form, provided that it is accessible for inspection by the FSA.*" This is further framed with a 48 hour notice period prior to inspection.

Do I have to retain any other paper documents?

It depends. However, in the vast majority of cases originals do not need to be retained. Some regulatory bodies may require specific key documents to be retained.

Although it's possible to scan any document into electronic format, the end image and eDM must conform to the following simple ground rules in order to be legally admissible or accepted by regulators:

- The document must be an exact replica of the original. It must mirror the original document in all legal respects no matter how many steps removed it is from an original paper document.
- The document must be of a high standard of legibility. There must be no ambiguity of interpretation introduced i.e. no modifications between it and the originating document.

A regulatory body may withdraw permission to present documents electronically if it is not totally convinced with the authenticity, integrity, legibility or timely availability of your electronic documents.

As a general rule of thumb, if you're not sure then seek guidance from your relevant regulatory body as the law in this area is complex and still evolving. For instance, staff personnel records need to be retained for six years after employment ceases and accident books need to be retained for three years after the end of each tax year for Statutory Sick Pay purposes. However, whilst the recommendation for Health and Safety records retention times is three years these are extended where employees have been exposed to hazardous substances.

Conclusion

Electronic filing is now increasing at such a level that it is commonplace for bodies such as HMRC to address the standards they require. Examples of best practice are increasing in organisations of all industry sectors.

The British Standard BS 10008: 2008 is the most comprehensive information available to businesses about best practice to follow to ensure legal admissibility of information. In complying with the Code, a business can be sure as possible that they are satisfying official record-keeping needs.

Before considering a eDM you should seek the advice of your relevant body and contact other companies already using eDM in your sector to ensure your choice of eDM builds regulation and legislation into your system from the start.

Postscript: Invu Document Management compliance

Invu Document Management is certified as BIP008 compliant. Scanned images are true representations of any original paper source and are tamper-proof through Invu's version control functionality. Documents are subject to a full unalterable audit trail. Access is covered by detailed in-built security functionality built into the product set. As we have seen, the operational working practices which your business implements play as important a role as the technology.

Disclaimer

This document aggregates a number of guidelines and good practices from regulatory bodies and document management vendors in the public domain. Whilst this information is created in good faith, and is understood to be correct at the time of writing, Invu accept no legal responsibility for information accuracy, loss or legal action suffered by businesses relying on the advice or information contained.

Invu would always advise consultation with a legal expert before destroying any paper documents.

Appendix 1

The legal admissibility of information stored on electronic document management systems

British Standards Institution (BSI) BIP0008
Code of Practice on Legal Admissibility and Evidential Weight of Information Stored Electronically

Introduction

The BSI Code of Practice is concerned with 'the authenticity, integrity and availability of electronically stored information, to the demonstrable levels of certainty required by an organisation. It is particularly applicable where this stored information may be used as evidence in disputes inside and outside the legal system'

ISO 15489 (BS ISO 15489-12001) is the international standard on records management. As there is overlap between the BSI Code of Practice and the International Standard the 2004 revision of the Code of Practice was to ensure that the two documents could be implemented together. The 2004 Code contains an annex mapping the content of the records management International Standard to the Code of Practice. The Code of Practice was originally published in 1996 as BSI DISC PD 0008. It was updated in 1999 as BSI DISC PD 0008:1999. The current Code of Practice is BSI BIP 008:2004.

Overview

The issue of Legal Admissibility is at the core of records management principles. An organisation needs to be able to prove (to a court of law or some other statutory body) that the contents of a particular document or data file created or existing within an Electronic Document Management System have not changed since the time of storage. If the data file is an electronically stored image of an original paper document, an organisation must be able to prove that the electronic image is a true representation of the original. Proving the authenticity of electronically stored documents is crucial to their admissibility in a court.

In England and Wales, the main statute governing the admissibility of documents is the Civil Evidence Act 1995. This Act resolved many of the outstanding legal difficulties that had arisen through the use of computers for information storage. The Civil Evidence Act shifted the argument from legal admissibility to evidential weight or value. It makes it easier to prove the authenticity of documents, by producing the original or a copy, irrespective of the number of removes between the original and the copy and irrespective of whether or not the document is a paper one or an electronic one. The court needs to be satisfied as to the authenticity of the copy, and therefore an organisation needs to be able to demonstrate that it has administrative procedures that will satisfy the court as to a document's authenticity. Irrespective of issues of legal admissibility or evidential weight, an organisation should ensure that the electronic storage of information complies at all times with best practice. As well as needing to meet legal requirements an organisation has business and ethical reasons for ensuring that the information it controls is not mishandled.

An organisation needs to demonstrate that it complies with the five principles of information management on which the Code is based. These principles are encapsulated into a code of practice - the "Code of Practice for Legal Admissibility and Evidential Weight for Information Stored Electronically" (BIP0008) published by the British Standards Institute. Compliance with BIP0008 will ensure that the organisation manages its information according to best practice, thereby maximising the chance of electronic records being satisfactorily authenticated.

An organisation will need to have in place the following five information management components:

1. Representation of Information (i.e. an information management policy)
2. A Duty of Care
3. Business Procedures and Processes
4. Enabling Technologies
5. Audit Trails

1. Representation of Information

An information management policy document will set out, for operating staff and any future litigants, the rules surrounding the various forms in which documents are held, the documents' life cycles and the legal advice sought and acted upon. The policy should set out in as much detail as necessary the variety of documents that will be presented for storage, for example: Internal and external correspondence, reports, drawings and specifications, legal documents and, perhaps, photographs, video and audio files. It will typically describe the different types of information held within the organisation and, for each type, specify:

- The level of security
- Appropriate storage media
- Formats and version control
- Information management standards, e.g. quality
- Retention and destruction policy
- Responsibilities and roles for information management functions
- Responsibilities for compliance with the code BIP0008

Any system needs to be flexible enough to satisfy the requirements of the organisation's information management policy. It must be capable of:

- Meeting the highest security standards set out in the policy
- Integrating with a wide range of storage media
- Handling different document types
- Managing documents under version control

- Meeting the retention requirements
- Meeting information management standards, e.g. storing images to the quality standard set out in the policy
- Allowing documents to be permanently erased

The 2004 Code recommends that a document management policy be developed, expanding on the retention schedule to include such details as media type, file format, destruction policy and responsibilities.

2. Duty of Care

To fulfil its responsibilities under the duty of care principle, an organisation will need to have in place:

- An awareness of the legislative and regulatory bodies pertinent to its industry
- A chain of accountability and defined responsibility for activities involving electronic document management at all levels
- A system to keep up to date with information management theory and practice, and developments among
- Appropriate bodies and organisations
- A documented information security policy

Under the duty of care responsibilities the system must have the functionality to allow for separation of roles. The person who inputs data should not be the same person who performs quality checks. This separation of administrative roles should be able to be mirrored in the logical access controls within the EDMS. The British Standard BS 7799: 1999 (ISO 17799) "Code of Practice for Information Security Management" is the UK/European reference document for information security. Proof of compliance with BS 7799 will usually demonstrate that an organisation has exercised a duty of care.

3. Business Procedures and Processes

An organisation should have documented operating procedures (a user manual) for each of the information management systems it runs. The procedure manual is the document that the organisation will produce, if it's electronic storage methods are ever challenged, to prove to auditors, lawyers or judges that the processes are precise, secure and approved for its normal business procedures.

The user manual will typically define the following:

- Document types
- Preparation of documents prior to scanning
- Photocopies
- Batch control
- Scanning processes
- Scanning specific documents
- Image Processing
- Compression Techniques
- How information is indexed
- Quality control
- Procedures for producing authenticated output
- Procedures for authenticating copies of documents
- How information is transmitted within the system
- Procedures for document retention and destruction
- System maintenance schedules
- Security and protection, including encryption and the use of digital certificates
- Backup and system recovery procedures
- Use of bureau services
- Workflow
- Date/time stamping
- Version control

It is important for the system to be able to produce output that will ensure that a document is appropriately authenticated.

The Code insists that the procedures and processes be audited annually, or more frequently for legally sensitive archives, to make sure that the approved procedures are being observed or that new ones meet the requirements of the Code and are formally and properly incorporated in the manual

Some specific recommendations in the code include:
Preparation of documents prior to scanning

The code requires that:

"Documents should be examined prior to the scanning process, to ensure their suitability. Such factors as their physical state (thin paper, creased, stapled, etc.) and the attributes of the information (black and white, colour, tonal range, etc.) should be noted. Procedures for this examination process should be documented in the user manual."

The Scanning Process
The Code requires, for example, that records be kept on the system audit trail of key information concerning imported documents. This information should include as a minimum:

- Unique identifier for each batch of documents
- Date and time of scanning
- Identity of the person who performed the scanning
- Type of material scanned (e.g. paper document, microfilm, aperture card, etc.)
- Number of documents and number of pages in each document scanned
- Detail of post-scanning processes (de-skewing, de-speckling, etc.) performed

The Code recommends that records be kept in batches so it is easier to check that:

- All required activity has been performed
- Any anomalies have been noted
- Appropriate quality procedures have been completed
- Records of any exception processing have been made

These batching recommendations allow a company to acknowledge that its system cannot be perfect, but that it has seen the anomalies and has registered them, either with a view to correcting them or merely making note of them. If the accuracy the system is challenged in court, the company will be able to it knows where mistakes are made.

Indexing
The Code makes the statement:
"Indexing is a vital part of the process of storing documents"

Whether the system involves automatic indexing, manual data entry, or a combination of these, the Code insists that:

"Procedures for indexing documents should be described in the user manual. These procedures should include methods of checking the accuracy of the index records created."

It sets out what should be recorded, what the audit trails should reveal and operator training requirements. It reminds the records management team to set realistic quality control criteria and processes for noting errors and levels of legibility.

Quality Control
It is important to be able to demonstrate to a court that quality controls are adequate and work. The Code sets out several important processes, including these:

"A sample set of original documents, or of documents equivalent in characteristics to the original documents, should be assembled for the purposes of bench-marking scanning system performance against the quality control criteria."

and

"The result of all quality control checks, including Test Target scans, should be recorded in the quality control log."

The records manager must test and check regularly and record the results of those tests and checks.

Document Retention
The Code says that all retention and destruction procedures should be recorded in the user manual. It sets out instances when, even if company policy is to destroy all documents after scanning, some papers may have to be retained:

- Where photocopies have been used to aid the scanning process
- Where the original is of poor quality and below the standard required by your system
- Where an original contains amendments that cannot be identified on a scanned image.

"No original source document should be destroyed until the write processes have been verified and appropriate backup procedures completed."

Originals should not be shredded until it is clear that the scanning and indexing processes have been completed properly and the data has been backed-up.

Security and Protection
Security and protection covers user access, mixed and/or removable media storage, file transfer protocols, data and hardware security, virus infection, power failure and auditing.

The Code states:
"Where mixed-media hierarchical storage systems are used, they should be assessed to ensure that they are used in a write-once mode only."

"Data file transfers, such as moving documents from one device to another, should be controlled by the application software. It should not be possible to move documents or change index data without an entry in the audit trail."

"Although the user facilities (document input and output) may be provided in a normal (unprotected) environment, the central part of the system (file servers, data storage, system software, etc.) should be installed in a secure area with restricted physical access."

4. Enabling Technologies

A typical system will be comprised of many different technologies. Each of these technologies, or rather their component parts, will need to comply with BIP0008. The Code describes technologies that may be used in a storage system and how they should be utilised and controlled to ensure that the system will store documents in accordance with BIP0008. These technologies include:

- Storage media
- Access control mechanisms
- System and data integrity
- Image processing
- Compression techniques
- Compound documents
- Data migration
- Document deletion

Each of these properties of an eDMS is critically important.

Storage Media
The issue of appropriate storage media is critical. There are two types of storage media, distinguished by the medium's ability to be written to many times or just once:

- Write many - or 're-writable' technologies
- Write once - commonly referred to as WORM ('write once - read many') technologies

An alternative way of considering data storage technologies is to distinguish between magnetic media and optical media. In general, magnetic media are write-many technologies while optical media may be write-once or write-many. CD-RW (CD re-writable) and erasable optical disks are optical technologies that can be written to many times. It isn't necessary to use WORM technology to comply with BIP0008. While WORM has the advantage that it is not possible to directly modify data once it has been stored, in practice data is modified by deleting the original data and writing the modified data. Each time a file is modified a new copy of the file has to be written, rather than just overwriting the existing file. The available storage space can be reduced much more quickly than expected. As WORM storage is more expensive than magnetic disk (and even RAID array), the use of WORM exclusively for storage can be expensive. Access to data on a WORM drive, particularly one in a jukebox, is slower than access to data stored in a RAID array. Data stored on magnetic disk can in principle be modified. However the risk of this happening, while significant, is small and the risk can be minimised, if not eliminated altogether, by ensuring that adequate controls are implemented in both the storage system and the eDMS access control system. Users with read only access rights cannot modify the data but those with read/write access obviously can, and therefore there is a requirement to securely log at the system level all read/write accesses so that unauthorised writes to the system can be detected.

Access Control
The system must have an adequate access control mechanism implemented so that individuals, groups and roles can be distinguished, and permissions granted based on the access control list.

System and Data Integrity
The system should provide an environment in which the integrity of the data is preserved, including the transfer of data between the eDMS software and the storage medium. Data integrity should be inherent to the eDMS and any integrity anomalies should be automatically detected and reported. Malicious attempts to change the data should be detected, though if the person acting maliciously has sufficient knowledge of the system's integrity checking mechanism, it might be possible for that person to alter a document and to 'fool' the integrity checking. Digital signature technology ensures that the integrity of a data file or a document in a system can be verified. A document that has been digitally signed cannot be altered without invalidating the signature. The eDMS software should be capable of working with the technology that implements digital signing. The signature also has a secondary role, one of non-repudiation - the person creating a document and signing it cannot subsequently deny authorship.

Compound Documents
A compound document contains a variety of parts - photographs, graphics, text, and video perhaps. It may be disassembled and each part processed in different ways. The Code advises that they be stored on the same storage device along with the metadata needed to identify the respective locations automatically and make an "accurate and unambiguous reconstruction" of the complete document.

Image Processing
Image processing is a post-scanning technique to improve the quality of a scanned document. These processes can include de-skewing, de-speckling, background clean-up, border, "noise" and forms removal. Though there can be good reasons for improving image quality, care must be exercised in image cleanup to ensure that essential detail is not removed. The Code warns that the techniques are used "with extreme care". De-speckling, for instance, carries a high risk of removing punctuation or decimal points. Any image processing should be identified in the system user manual. Any image processing techniques used could reduce the evidential weight of subsequent retrieved images.

Compression Techniques
Systems storing scanned images normally use compression algorithms to reduce file sizes so that storage requirements are reduced and system performance improved. It is important to ensure that images, when compressed, are not subject to data loss. If the compression technique is a 'lossy' one (for example storing an image as a JPEG) then detail necessary to authenticate the stored image may be lost, reducing the evidential weight of the image. If lossy compression is used, a sample set of scanned images should be made to check and approve the level of information loss. Lossy compression should not be used for documents containing primarily text, but may be more acceptable with photographs.

Data Migration
A system should have the ability to migrate documents and data to some to other hardware/software platforms and other storage media. Documents, such as personnel records, may have a lifetime longer than the current system and therefore at some point will need to be migrated. The system should use open or industry standards for data storage rather than proprietary ones.

Document Deletion
To meet the requirements of Privacy or Data Protection Acts, it may be necessary to amend or delete documents, or parts of documents. This might occur routinely, as part of the organisations' retention policy, or exceptionally as a result of legal or regulatory requirements. Note that a WORM ('write-once, read-many') storage medium could make this operation difficult. The Code sets out acceptable methods - use of masks, index entry cancellation, document replacement, etc. – which should be identified in the user manual and whose use must be recorded in the system audit trail. See the "Guide to the Data Protection Act" for further details.

5. Audit Trails

BIP0008 requires that a system must have full auditing functionality. Without detailed audit trails (i.e. a record of a document's life history) authenticating a document, and therefore satisfying a legal body, may not be possible. In addition, irrespective of legal requirements, an organisation will require audit trails to meet its own managerial requirements, such as internal audit. The audit trail, as a minimum, should log details of each significant event in the life of a document in the system.

The audit trail should:

- be generated automatically by the system
- contain date/time stamps for each event

- be non-alterable
- be stored in accordance with the organisation's information management policy
- be subject to appropriate access control
- be securely stored and backed-up

The system should be able to provide an enquirer, with appropriate permissions, (even one unfamiliar with the processes) access to the full audit trail record and, preferably, have a reporting tool to allow production of customised reports from the trail. There is also the issue of retention periods. If documents are kept for, say, seven years, then it is likely that you will need to keep audit information for at least seven years also.

Compliance with the Requirements of the Code of Practice
To assess the current status of compliance with the requirements of the Code of Practice, the BSI publish a Compliance Workbook (BIP 0009). This Workbook consists of a series of questions, each of which needs to be reviewed and answered. Typically, it takes one to three days to complete the Workbook for the first time. Some investigations may need to be carried out on particular issues, which may lead to more time being needed. There may also be a need to consult with the system supplier. Typical most of the compliance points are addressed by implemented systems. Compliance points that are often missing from systems include:

- No Information Policy document
- No retention schedule
- Inappropriate security controls
- Lack of procedural documentation
- Insufficient control on document input procedures
- Insufficient information about the technology from the system supplier
- Use of inappropriate facilities, such as image clean-up
- No thought of future migration requirements
- Lack of documentation on audit trail content and access procedures.

Each of these could potentially compromise the ability to demonstrate the authenticity of the stored documents.

Compliance Workbook (BSI PD0009)
The British Standards Institution Compliance Workbook (PD0009) is available to aid implementation of the Code. Its pages parallel those of the Code, reminding and instructing systems managers what to undertake. All questions have a Yes/No tick box to ensure compliance.

Principles of Good Practice (BSI PD0010)
The Image and Document Management Association (IDMA) Principles of Good Practice for Information Management, PD0010, is published by the British Standards Institution as the third in its "legal set" of guidelines. It is "Intended to help those who have responsibility for assisting their employers to develop and operate new methods …"

Appendix 2

Additional reading

- http://www.ukaiim.org/publications.htm
- http://shop.bsigroup.com/en/ProductDetail/?pid=000000000030191165

About the Author

Mark Palmer is Director of Product Management and Marketing at Invu. Since joining Invu in 2008 he has worked with the Invu partner channel and established customer product forums. Together with Invu's CTO Stuart Evans, he oversees the future of the Invu product set and its delivery to market.

Before joining Invu. Mark has worked in product management roles at Ceridian and Sage, where as head of Product Management in the Accountants Division he was responsible for products for the UK accountants market. Prior to this Mark worked on a series of software delivery projects, notably at the 2002 Manchester Commonwealth Games. Having started off in the accountancy profession Mark has over 20 years of experience in the software industry as analyst, project and product manager.

About Invu

Invu develops software that incorporates document management, content management, workflow, automation and collaboration. Also known as the paperless office, Invu typically gives a Return on Investment in under six months, allowing companies to see efficiency savings in terms of both money and time. Invu specialises in solutions for the mid market and smaller businesses.

Invu's Open Search integration allows SharePoint users to fully utilise the benefits of WSS or MOSS whilst retaining the functions of specialist document and content management.

Invu's solutions enable automated scan, capture and management, processing and output transformation. Invu also integrates with all major accounting systems including Sage and IRIS, as well as ERP and CRM systems.

Further Information

Press & PR enquiries

Invu

Naomi Edwards

comment@invu.net

01604 859893