

» Moving to a Paperless Office - Is it Just About the Cost of the Technical Solution? «

A white paper by Angela Isom,
Siemens Insight Consulting



There is growing evidence that organisations are increasingly moving from paper audit trails to paperless office environments - after all, they can provide huge savings to a business through reductions in storage requirements, reduced costs in locating records and easier retrieval of information. Sounds simple and a convincing business case.....

Document scanning, electronic storage solutions, Intranet and internet sites can all provide opportunities for quicker, cheaper and easier retrieval of information than when it's held in paper format but the question remains— is it just about finding a document record management system or are there other issues to consider when moving to a paperless environment?

Why do organisations retain so much paper?

Legal and regulatory requirements demand that organisations retain a significant number and variety of records in the form of contracts, transactional records, employment records, accounting data, research data and in some cases correspondence. Traditionally, this type of information held in original paper format including contracts with original signatures, have all been accepted in a Court of Law as proof of an evidential record.

What is the legal basis to move to a paperless office?

So, what is the Court's view on whether any of these paper records can now be held within an electronic storage solution? Well, the Civil Evidence Act 1995 provides that copies of information don't need to be in their original form in order to be treated as evidence in a Court of Law. Whether a copy of an original document will be considered as evidence is largely based upon its authenticity, i.e. proof (an audit trail) that it has not been tampered with and that it still retains its integrity as an original record.

Likewise, UK Courts now recognise the legality of electronic contracts and signatures (as a result of the Electronic Communications Act 2000). In general, the key objective of a written signature is to demonstrate that an individual intended to take up a contract and understood the terms and conditions. The functions provided by the written signature can be achieved using a series of technical controls and electronic signatures.

The issue that presents a challenge in the absence of direct case law is the level of interpretation around the amount of information required to establish the facts around electronic contracts and signatures should it be required to be resolved in a Court.

So, the challenge now moves on to how integrity of original paper documents, as well as the authenticity of electronic signatures and contracts can be ensured when using an electronic storage solution, i.e. how to prove integrity to a Court of Law.

Can organisations get rid of all of their paper then?

Not quite - a number of documents/contracts must be expressed in a paper representation only, namely:

- Documents dealing with family matters such as wills, divorce and adoption
- Notices dealing with the consequences of late or non-payment or the termination of an agreement
- Court documents
- Product recall notices
- Notices sent with hazardous materials
- Original paper records of VAT records. These need to be retained for no less than one VAT period for inspection by the VAT office. After a VAT return has been submitted, the original VAT records can then be scanned and filed electronically within the document record management system
- Original vouchers for tax deducted or for tax credits.

What can organisations do to prove integrity to a Court?

The Courts are leaning towards those organisations showing compliance with BSI DISC PD0008, the British Standard which relates to the Legal Admissibility of Evidential Information Stored Electronically. It provides a framework and guidelines that identify key areas of good prac-

tice for the implementation and operation of electronic storage systems, whether or not any information held therein is ever required as evidence in event of a dispute. As such, compliance with this Code of Practice is regarded as a demonstration of responsible business management, although it doesn't guarantee legal admissibility.

The Code revolves around Five Principles:

1. Information Management Policy

Development and approval (at a senior level) of an Information Management Policy covering the Code's specific requirements for Protective Marking, Approved Storage Media Policy, Data File Formats (there is considerable information in the Code about how documents are to be scanned including document image quality), Disposal Policy, Data File Formats Policy as well as quality system processes to govern compliance.

2. Duty of Care

Development and implementation of an Information Security Policy, an Information Security Management System (ISMS), version control of all information types with date and time stamps as well as Data Retention and Disposal Policies in compliance with the Data Protection Act, are required.

As the Standard isn't a legislative or regulatory requirement, compliance is carried out on a risk based approach to determine the threats, impacts and vulnerabilities mapped off against the appropriate countermeasures needed to be implemented. An effective Prince 2 compliant Risk Assessment Methodology should be used, such as CRAMM, and the implementation of the recommended countermeasures carried out and monitored as part of the ISMS auditing cycle.

The Code is concerned with the authenticity and integrity of Original Documents and has numerous recommendations surrounding images, macros and paper records and how they enter the electronic storage solution. These requirements must be built into the associated functionality of the solution, which itself should meet the requirements of the Standard for Records Management, BS ISO 1549.

3. Procedures and Processes

The Code is highly geared around the identification, development, implementation and maintenance of processes such as data capture and migration requirements, indexing and authentication of outputs to support the policies in 1 and 2 above. These all need to be available in a central repository of policies and procedures, subject to formal change control, which must be easy to read and lend themselves to training staff on how to apply them.

4. Enabling Technologies

Choosing a reliable and trustworthy electronic storage solution is essential. It must be capable of supporting access to the records based on the 'need to know principle' to ensure compliance with the Data Protection Act 1998. As such, role segregation and a Role Based Access Control Schema should be created, maintained and complied with. Integrity and

availability of data are key themes within the Code. Platform hardening standards should therefore be implemented, audit data trails maintained to allow for reconstruction of evidential records, cryptographic requirements appropriately implemented and monitored, and contingency plans developed, implemented and tested.

5. Audit Trails

Audit trails are essential to provide a trustworthy record of the operations that have been performed on data stored within a document record management system. Logs of suspicious activity and of every access to any record and/or modification made to any data contained within the electronic storage solution should create an audit trail showing who made the changes, at what time and what the before and after data values are. Audit data should be stored on Write Once Read Many (WORM) systems (optical media is preferable) in an encrypted form (or be the subject of Checksums to provide legal assurance of audit data integrity) but these shouldn't be on the same system from which the audit data is derived.

Compliance with the Code isn't impossible – but it requires ongoing demonstrable auditing to prove the integrity of the records contained within it. HM Revenue and Customs use PD0008 as the basis of their requirements for scanned documents to meet their specific requirements for both VAT and Tax records.

Is it as simple as complying with PD0008?

It's a nice thought, but no, it isn't that simple. It is an effective starting point and should be considered before choosing any electronic document storage solution. Organisations also need to consider the following:

- **Data retention and disposal requirements** - derived from legislation including data weeding and disposal to ensure that destruction of data is secure and that evidential probity of scanned documents has been assured prior to hard copy data destruction
- **Audit data requirements** - to meet ISO 17799, evidence legislation and the Data Protection Act 1998
- **Access control considerations** - to ensure compliance with ISO 17799, evidence legislation and the Data Protection Act 1998
- **Interface requirements** - including encryption and safeguarding of encryption keys
- **Backup obligations** - to ensure use of optical WORM devices for legal integrity of data with 0% data loss to prevent loss/corruption to ensure compliance with the Data Protection Act 1998 and evidence based legislation
- **Disability Discrimination Act requirements** - to ensure that the solution meets the needs of disabled users
- **ISO 17799** - evidence of compliance with this standard assists in showing a Court that the computer records can be relied upon

- **Auditing the auditors** - who is auditing the system administrators? Checks need to be in place to ensure integrity of data or all other controls can be called in to question by a Court of Law
- **Testing** - the electronic storage solution and ongoing patches to it will need to be tested including IT health checks before they are operated within the live environment - they shouldn't be tested using live data
- **Clock synchronisation** - the electronic storage solution's application clock needs to be synchronised with those with the organisation's estate to ensure that audit data is consistent and reliable
- **Monitoring** - users that send information to or receive information from the solution must consent to and/or have been advised that interceptions of their communications may be made without notice
- **Freedom of Information Act 2000** - the storage solution will need to support swift and easy searches for information
- **Technical and organisation controls** - derived from legislative requirements
- **Printing of Evidential Records** - all data contained within the electronic storage solution should be capable of being printed to produce a permanent record accompanied by authentication of the data, i.e. a digital signature proving the integrity of the original file by showing that it hasn't been tampered with and that it will satisfy the test of repeatability, i.e. it will create the same output of data every time.

Summary

The business benefits of moving from a largely paper based system to an electronic storage system (paperless office) are clear, but there are a significant number of issues that organisations should consider to ensure that their procurement of an electronic storage solution and its deployment meets their internal business needs and legislative requirements, as well as allowing them to retain the capability to produce evidential records recognised by our Courts of Law. The accuracy and provenance of the original data must be scrutinised before there is any destruction of original hard copy files. All requirements of PD0008, the Civil Evidence Act 1995 and the Criminal Justice Act 2003 need to be considered in terms of maintaining the evidential probity of the evidence.

Moving to a Paperless Office - Is it Just About the Cost of the Technical Solutions?

A move to a paperless office isn't therefore as simple as first thought, but meeting these challenges will not only achieve the business benefits organisations initially anticipated, but will also provide a far more secure working environment in general, which will reduce the risk of security incidents and failure to comply with an organisation's legislative obligations.

Insight Consulting, part of Siemens Communications – a division of Siemens plc (Insight) is a specialist in the provision of information security, continuity and compliance consultancy services and can assist organisations in meeting their business objectives in moving to a paperless office whilst appropriately considering all of the issues identified in this paper. Our services include both organisational and technical solutions.

If you would like further information or to discuss the topics raised within this white paper, please feel free to contact Angela Isom who manages Insight's Legal and Regulatory Compliance Consultancy team via insight@insight.co.uk or phone 01932 241000.



Author's biography

Angela Isom is a Senior Consultant at Insight Consulting with over 9 years experience in a compliance role.

Angela specialises in compliance with the Data Protection Act 1998 (DPA), the Freedom of Information Act 2000 (FoIA), related legislation and best practice information security principles to BS 7799 standards. She is Insight's Data Protection Officer and has considerable hands-on experience of implementing best practice controls as well as writing, and being responsible for, the associated information security policies and procedures.

Angela regularly conducts Data Protection compliance audits and document reviews for her clients culminating in security improvement programmes that, when followed, afford clients with ongoing compliance programmes for both Data Protection and best practice information security management. Angela provides application legal and security frameworks to drive the design and audit of applications to meet both best practice security requirements and the extensive legal requirements placed on Data Controllers.

Insight Consulting is the specialist Security, Compliance, Continuity and Identity Management unit of Siemens Communications and offers a complete, end-to-end portfolio encompassing:

- Security
- Continuity
- Managed Services
- Compliance
- Identity Management
- Training

Siemens Insight Consulting subscribes to the CESA Listed Advisor Scheme (CLAS) and CHECK services. We're also certified against BS7799 and are a preferred supplier of services to the UK Government and are an accredited Catalyst supplier.

If you'd like to find out more about how we can help you manage risk in your organisation, visit our web site at www.siemens.co.uk/insight
Siemens Insight Consulting
Tel: +44 (0)1932 241000
Fax: +44 (0)1932 236868

www.siemens.co.uk/insight