Preparing for corporate information and records management: a guide to best practice

4.1 Coverage

In this chapter we review some of the key steps that should be completed to ensure that an organisation is ready to make the move to electronic information and records management and collaborative working (Fig. 4.1). The recommendations are based on good practice, guidelines and standards, and on Cimtech's more than twenty years' experience of assisting clients with the implementation of enterprise content management and electronic records management solutions.

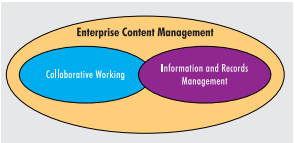

Fig 4.1
Enterprise content management framework

Section 4.2 makes the case for improving corporate information and records management, and for managing information as a corporate asset. Section 4.3 looks at what is involved in agreeing a corporate information management and records management policy, and the benefits that they can bring. Section 4.4 reviews best practice guidelines and standards.

4.2 The Case for Information and Records Management

Fig 4.2
Information is a strategic asset

For organisations, the information they possess is a strategic asset (Fig. 4.2). Without that they would find it difficult or impossible to operate. This information has a very high value equal to or, in many cases, exceeding the value of staff or capital assets.

However, many organisations do not really understand those information assets and are not harnessing or exploiting them to their full potential. Even worse, in many cases they are not even protecting them, so they are vulnerable to loss or theft.

This is despite the fact that over a decade ago the influential Hawley committee published a report called *Information as an asset: the board agenda*[1]. The report proposed that all significant information in an organisation, regardless of its purpose, should be properly identified, even if not in an accounting sense, for consideration as a business asset. The board of directors, it argued, should address its responsibilities for information assets in the same way as for other assets, e.g. property and plant. This implies that a new approach to information management is required.

The board should satisfy itself that: the information it uses is necessary and sufficient for its purpose, it is aware of and properly advised on all the subjects on its agenda, its use of information, collectively and individually, complies with applicable laws, regulations and recognised ethical standards.

To determine the quality and quantity of information needed for effective operation many organisations are taking a functional view of their activities. They are reviewing the information required at each stage of each process in the business to ensure that necessary and sufficient information is available for effective operation – and no more. Too much information can be as bad, or even worse, than not enough information. They are defining roles and responsibilities with regard to information. Best practice calls for a clear distinction to be drawn between its owner (responsible for creation and accuracy), the custodian (responsible for physical safekeeping), those with right of access (who can view but not change information), those with the right to copy (who can reproduce information for other purposes) and those with the right to destroy (who can eliminate all traces of information).

Records management is a vital subset of information management and today there are international standards and guidelines designed to assist organisations in formulating and implementing standard records management policies and procedures.

International Standard 15489:2001 *Information and documentation – Records Management*[2] is a two-part standard. It emphasises that standardisation of records management policies and procedures ensures that appropriate attention and protection is given to all records and that the evidence and information they contain can be retrieved efficiently and effectively using standard practices and procedures.

The standard was developed in response to consensus among participating ISO member countries to standardise international best practice in records management using the Australian Standard AS 4390 *Records Management* as its starting point. It defines the objective of any corporate records management policy as being "the creation and management of authentic, reliable and useable records, capable of supporting business functions and activities for as long as they are required".

The corporate governance of information assets

The board should determine the organisation's policy for information assets and identify how compliance with that policy will be measured and reviewed, including:

- The identification of information assets and the classification into those of value and importance that merit special attention and those that do not.
- The quality and quantity of information for effective operation ensuring that, at every level, the information provided is necessary and sufficient, timely, reliable and consistent.
- The proper use of information in accordance with applicable legal, regulatory, operational and ethical standards and the roles and responsibilities for the creation, safekeeping, access, change and destruction of information.
- The capability, suitability and training of people to safeguard and enhance information assets.
- The protection of information from theft, loss, unauthorised access, abuse and misuse, including information which is the property of others.
- The harnessing of information assets and their proper use for the maximum benefit of the organisation including legally protecting, licensing, re-using, combining, re-presenting, publishing and destroying.
- The strategy for information systems, including those using computers and electronic communications and the implementation of that strategy with particular reference to the costs, benefits and risks arising.

4.3 Developing Information and Records Management Policies

4.3.1 Information management policy

Since the work of the Hawley Committee was published a number of organisations have developed their own corporate information

Example information management policy

- Internal information is owned by the company. All information will have a defined custodian who, as the authorised agent of the company, will be responsible for its management and for making it available to those who need it.
- Information will be managed to support business processes rather than organisational hierarchies.
- Information will be managed, accurate and up-to-date and will be readily accessible to those who need it.
- Information will not be retained or distributed unnecessarily.
- A consistent approach to managing information will be adopted across the whole company and will cover the lifecycle of information (creation, indexing, storage, retrieval, revision, archiving/disposal).
- Methods of information management will give due attention to security, protection, legal, environmental and cost issues.

management policies (Fig. 4.3). A good policy should be short and concise so it can be read and memorised by all employees. One policy developed at the time comprised six key points.

The first point is very important as it establishes that information and records management is everyone's responsibility. If a user creates information/records while being paid by an organisation they have a responsibility to ensure it is adequately managed.

The second point is echoed in many best practice guidelines.

The third point is easy to agree but hard to deliver. It should be a core business objective. If it is, then it becomes relatively easy to justify electronic systems as without them the task of keeping information accurate, up-to date and readily accessible is extremely labour intensive.

The fourth point addresses legal and efficiency issues. Organisations need to take account of data protection issues and should avoid copying and duplicating activities, which do not add value but consume considerable resources.

The fifth point is vital and electronic records management (ERM) and process automation offer the tools to achieve such consistency, but the stages in the lifecycle need to be defined.

The sixth point echoes the need for compliance with good practice and legislation. The BSI *Code of practice for legal admissibility and evidential weight of information stored electronically*[3] recommends organisations adopt an information management policy.

In order to ensure that this information is well managed, and to meet its business needs, the organisation needs to define and implement good management practices. Information, like any other asset, needs to be classified, structured, validated, valued, secured, monitored, measured and managed efficiently and effectively. To provide guidance to those who have the responsibilities of these practices, the senior executives need to approve an information management policy statement.

Chapter 1 of the BSI code outlines the content and approval recommendations for the policy statement and is recommended reading. Annex E of the code includes an example policy document that may be used during the drafting of an organisation's policy document. The code recommends that the policy document should contain, as a minimum, the following sections:

4.3.2 Records management policy

Many organisations, especially in the public sector, have produced their own records management policy. Guidance on how to develop an overall policy is provided in the ISO 15489[2] and by bodies such as The National Archives (TNA). Based on this guidance most policies are relatively concise documents structured around ten to twelve headings. The following headings have been used by Cimtech when developing RM policies for clients:

Section	Content
Information covered	Specifies which information 'types' are covered by the policy.
Security classification	States the policy regarding security classification (where used).
Storage media	States the policy regarding the type of media to be used for storage.
Data file format	States the policy regarding data file formats and version control.
Standards	States the policy regarding relevant information management standards.
Retention schedule	Defines retention periods and disposal policies.
Responsibilities	Defines responsibilities for information management functions and for compliance with the Code.
Consultations	Includes or references the results of consultations with appropriate legal and/or regulatory bodies and with others where necessary.
Auditing	Defines requirements for auditing relative to particular document 'types'.

Fig 4.3
Developing effective corporate information and records management policies is vital

Section	Heading
1	Purpose
2	Policy statement
3	Scope
4	Policy context
5	Legislation and standards
6	Records management systems
7	Responsibilities
8	Promotion
9	Training
10	Review
11	Authorisation
12	Glossary

Purpose This section should define its key aims. In the public sector typical aims would be to ensure that the authority:

- Has appropriate records to meet its business needs and the needs of its stakeholders
- Operates records management procedures and practices that conform to applicable legislative requirements
- Clearly defines responsibilities and accountability for records
- Provides staff with the resources, knowledge, competences and procedures to manage records according to the policy
- Addresses its obligations under Freedom of Information legislation to have a policy in operation for records management.

Policy statements These need to be supported by detailed standards and procedures explained in a records management guide, and by a programme of staff training and communication. The policy statement should be short and sharp and commit the organisation to maintaining all the records it needs and is obliged to keep. One example follows:

The authority will document its business activities with records that are complete, authentic, reliable, secure and accessible and manage those records in accordance with all applicable legislative requirements throughout their lifecycle.

Fig 4.4
The scope of the RM policy may include paper records as well as electronic records

Scope The scope of the policy will define the range of records covered and generally will indicate that the new policy covers both paper or analogue records (Fig. 4.4) and electronic records in all formats. It will refer to a list of records if such a list has been produced as a result of an audit and it will cover any exclusions.

Policy context This should refer to other relevant documents. This may include the information management policy and strategy of the organisation.

Legislation and standards This should list all legislation that has an impact on the records that must be kept and all standards the authority is committed to following. These would include relevant Acts of Parliament, codes of practice and standards.

Records management systems This section should specify a minimum set of requirements for systems and processes that manage records. It may list all the core processes covered and should refer to separate detailed procedures for the management of paper and electronic records and indicate where they are held.

Responsibilities This section should indicate generic and specific records management responsibilities within the organisation including senior management, records management and information management staff, managers and supervisors and all staff.

Promotion The section should explain how the policy will be implemented in practice and how the policy will be communicated to all employees. Detailed implementation procedures will be included in the guide. Any project to implement an ECM solution should include a communications plan designed to ensure all employees are informed about the project and kept up-to-date on the status of the project and their responsibilities.

Training This section should explain how all levels of staff will be trained to ensure records management responsibilities are met.

Review This section will commit the organisation to reviewing the policy on a regular basis and will task a committee with that responsibility and define he criteria it will be reviewed against.

Authorisation This section will state that the policy has been authorised by senior management.

Glossary This will contain key definitions including what is meant by a record. There are many such definitions. A useful one provided by The National Archives is as follows:

"A record is a specific piece of information produced or received in the initiation, conduct or completion of an institutional or individual activity. It comprises sufficient content, context and structure to provide evidence of the activity. It is not ephemeral – that is, it contains information that is worthy of preservation in the short, medium or long term."

Many existing records management policies cover only paper records but increasingly any overall policy should include electronic records. Extracts from The National Archives draft corporate policy on electronic records[4] are provided below. The overall policy should make it clear that electronic records are covered by the policy and state that all systems and processes that deal with electronic records must ensure that the records are managed in line with the overall records management policy.

The National Archives Corporate Policy on electronic records is aimed at departmental record officers and other personnel charged with records management in public sector organisations. The aims set out for the policy in Section 1, Summary, are to:

- Provide clear guidance on what electronic records are and why they need to be kept
- Explain how good ERM serves major needs of the department
- Set out generic principles and policies on specific aspects which form the basis of implementation
- Define responsibilities for records throughout the organisation.

Section 2, Introduction, places the document in the context of the wide range of guidance documents produced by The National Archives. It explains why a policy for ERM is needed. The policy should ensure that:

- The record is present
- The record can be accessed
- The record can be interpreted
- The record can be trusted
- The record can be maintained through time.

These are key objectives for all records – analogue or electronic – and should be included as aims in any general records management policy as well. The National Archives point out that the first three items are commonly found in a general organisational information policy, aiming to ensure that:

- The right information is captured, stored and preserved according to needs
- It is fully exploited to meet current and future needs and to support change and development
- It is accessible and meaningful in the right format to those who need to use it
- The appropriate technical, organisational and human resource elements exist to make this possible.

The National Archives further points out that the remaining items (trustworthiness and permanence) carry special implications for records and influence the way in which the first three can be implemented. In order to achieve these qualities for electronic records, formal policy statements can offer the corporate authority and institutional guidance, which records managers require.

Section 3 reviews how organisations should plan the development and adoption of the policy.

Section 4 defines the overall coverage of the policy.

Section 5 covers the policy framework. The National Archives makes the point that the policy may be merged within a general corporate policy for records or kept separate. Maintaining the effectiveness of the policy means the interaction between the electronic records policy and other policies should be stated. The following examples are cited by The National Archives and could be added to: following best practice (ISO 15489, PD 0010, etc.), the department's e-business strategy, freedom of information, data protection and existing records policy.

The National Archives Corporate Policy (document breakdown)

Section 1	Summary
Section 2	Introduction – providing a context
Section 3	Planning the policy
Section 4	What a policy should cover
Section 5	Policy framework
Section 6	Implementing the policy
Section 7	Technical policy
Section 8	Preservation policy
Section 9	Registration policy
Section 10	Access policy
Section 11	Security policy
Section 12	Policy review

Section 6 covers implementation. The policy should be communicated from the top of the organisation in a summary form that everyone can understand. The full policy should be provided to people who have a part to play in its implementation and further development. Procedures will need to be developed later in line with the policy and embedded in the ways people work. Effective records management is one element within corporate information management and should be co-ordinated with and contribute to the development of the information management strategy.

Section 7 covers the technical policy and should establish the criteria to be applied to the technologies that process electronic records. Government and individual organisations' IT strategies will set requirements for the IT systems in more general terms.

Section 8 covers the preservation policy needed to ensure that electronic records are visibly present and maintained in an authentic state. The technology that serves to process the electronic record will change over time, but the preservation policy should seek to minimise the risks associated with any technological changes and ensure that the records remain intact.

Section 9 – the registration policy – should help the organisation to set minimum conditions for the registration of electronic records. The registration policy should be broad enough to standardise registration systems so electronic records are well organised and can be discovered by a third party. It should not be so restrictive that the records are arranged or labeled in a cumbersome way and thus slow down operations.

Fig 4.6
A number of published guides are available covering best practice

Section 10 is the access policy, which should control the movement of information in and out of the records management systems, allowing the records to be created or viewed by different categories of users.

Section 11 – the security policy – should build confidence in the management of records. It should protect the records management infrastructure as well as safeguard individual records from interference and misrepresentation.

Fig 4.5
Policies need to be reviewed regularly

Section 12 covers the review of the policy. A policy review should happen on a regular basis and can increase the effectiveness of the policy by establishing how it is interpreted within the organisation and suggesting changes where there is uncertainty (Fig. 4.5).

This is a very useful document, which can be found in the records management area of The National Archives website[4] alongside other relevant guidance documents.

4.3.3 Implementing the policies

It is not sufficient simply to agree an information and records management policy. The next challenge is to implement that policy. Some of the key components needed to successfully implement information and records management are listed below.

One of the key tasks to be carried out by an organisation is to benchmark its current corporate information and records management policies, procedures and systems against best practice guidelines. Chapter 5 summarises Cimtech's preferred methodology for improving policies and procedures and specifying and implementing a corporate ECM solution. It is based on the EDRM System Implementation Toolkit(5) which Cimtech developed for the Joint Information Systems Council (JISC) and which can be broadened out to cover a full ECM implementation.

The key components for a successful information and records management policy

- An information management policy, which must be supported by senior management and be widely publicised.
- An individual or a team in a large organisation tasked with the implementation of the policy and reporting back to the board. In a large organisation the team should comprise senior staff from information systems, the library, the records management section and external independent consultants such as Cimtech and others listed in the Directory section.
- A strategy for implementing the policy – for defining the overall information management requirements, the objectives and the framework for integrating the organisation's information resources, services and systems.
- As a result of the strategy, standards, procedures and controls for the acquisition, storage, processing, distribution and disposal of information in all its forms.
- As a result of a successful strategy the information systems needed to support the real business needs.
- As a result of a publicised policy and senior management support a general awareness among staff of the real costs and value of corporate information, i.e. the value of the information asset.

4.4 Best Practice for Information and Records Management

There are a number of published guides and standards for best practice in information and records management (Fig. 4.6). Below we review briefly what we consider to be some of the key documents and list standards and other guidance documents.

4.4.1 Principles of good practice

BSI DISC PD0010[6] *Principles of Good Practice for Information Management* was authored in 1997 by Bill Mayon White and Bernard Dyer of the Image and Document Management Association (IDMA). It is designed to present a set of proposals or principles. The introduction defines the audience for the principles: "They are intended to help those who have the responsibility for assisting their employees to develop and operate new methods and techniques for managing information, and in particular that information which is stored and managed as documents."

There are five main principles. These are intended to act as guidelines for a set of procedures that any organisation should be capable of devising and operating as an extension of their current operating procedures, or of their quality management processes.

4.4.1.1 Recognise and understand all information types

The key objectives here are "the identification of information assets and the classification into those of value and importance that merit special attention and those that do not. You need to identify all your information, classify it and then index your information and record how it is represented".

They also state that organisations should choose "appropriate methods to capture, store and transmit information", which is similar to the fourth point in the policy above. Organisations need to establish the concept of lifecycle management and agree a consistent approach to managing information.

4.4.1.2 Understand the legal issues and execute duty of care responsibilities

This ensures that all staff are aware of relevant regulations governing information management and record keeping and then ensuring that everyone understands their responsibilities.

The five principles of good practice for information management

- Recognise and understand all types of information
- Understand the legal issues and execute duty of care responsibilities
- Identify and specify business processes and procedures
- Identify enabling technologies to support business processes and procedures
- Monitor and audit business processes and procedures

4.4.1.3 Identify and specify business processes and procedures

This section represents an extension of the requirements of the ISO quality standard BS EN ISO 9000 *Quality management and quality assurance standards*[7]. In order to understand information management requirements, and requirements for new electronic systems, the business processes need to be understood. Whereas they would have been documented in procedure manuals for ISO 9000 compliance we can now use process modeling software.

Equally, of course, the business processes can be improved and remodeled to take account of the fact that the introduction of electronic document, records and content management systems will mean that processes can be changed and streamlined.

4.4.1.4 Identify enabling technologies to support business processes and procedures

The objectives are to identify appropriate technologies to support and enable business processes. The authors wisely caution the user to establish procedures to monitor and control exposure to risks arising from the misuse or failure of its computer systems. As the technology becomes ever more sophisticated the need for contingency should always be considered.

4.4.1.5 Monitor and audit business processes

The final principle is that organisations should monitor and document their operations and any deviations from standards. In particular, any system implemented should be capable of providing audit trails for all information and documents.

4.4.2 ISO 15489-1:2001 Information and documentation – Records Management

A more recent British and International Standard is also extremely relevant here. ISO 15489:2001 *Information and documentation – Records Management*[2] was issued in two parts in 2001 in order to standardise international practice in records management using the Australian Standard AS 4390 as its starting point.

It is recommended for organisations that are setting up a records management programme or for those that need to audit existing policies, procedures and systems prior to developing a records management strategy and/or specifying requirements for an ECM solution. However, it should be clearly understood that ISO 15489 does not comprise a set of requirements for a records management system (paper based, hybrid or electronic). The National Archives and MoReq requirements address that.

Part 1 of ISO 15489 provides general guidance to managers on establishing records management policies, procedures and systems. It defines a comprehensive programme, which includes determining what records should be created and what information should be included in the records, what metadata should be created with the records and how they should be organised.

It recommends that a records management strategy should be documented in a strategic plan, such as an information management strategic plan, which should be incorporated into organisation-wide planning documentation. It defines the high-level requirements for a records system and outlines recommended records management processes and controls.

Part 2 is an implementation guide for use by records management professionals. It provides one methodology that will facilitate the implementation of ISO 15489-1 in all organisations. It includes an eight-point plan for designing and implementing a records system based on the Australian DIRKS (Designing and Implementing Recordkeeping Systems) methodology. This is a clear and concise document and is now forming the basis for a range of courses aimed at users who need to set up a corporate records management plan.

ISO 15489:2001 eight-point plan

- Conduct preliminary investigation
- Analyse business activity
- Identify requirements for records
- Assess existing systems
- Identify strategies to satisfy requirement
- Design records system
- Implement records system
- Conduct post-implementation review

4.4.3 ISO 23081–1:2006 Information and documentation – Records management processes – Metadata for records – Part 1: Principles

The first part of this standard[8] was revised by workgroup TC 46/SC11 and published in 2006. It is a further extension of the ISO 15489 records management standard to help people understand, implement and use metadata within the framework of ISO 15489. It addresses the relevance of records management metadata in business processes and the different roles and types of metadata. It does not define a mandatory set of records management metadata to be implemented, since these metadata will differ in detail according to organisational or specific requirements for jurisdiction. However, it assesses the main existing metadata sets in line with the requirements of ISO 15489.

This first part of ISO 23081 sets a framework for creating, managing and using records management metadata and explains the governing principles. The proposed future Parts 2 and 3 will be more explanatory and provide practical guidance on implementation issues and how to assess records management metadata sets against the principles in this part of ISO 23081. These future parts will be Technical Reports that should be considered as more time-bound documents that will need regular updates.

We will review these later parts as soon as they are published in the 2008 edition of this publication or earlier in *IM@T.Online*.

In a records management context, metadata is data 'describing the content, context and structure of records and their management through time'. As such, metadata is structured or semi-structured information that enables the creation, registration, classification, preservation and disposition of records through time and within/across domains. Part 3 will provide an assessment of existing metadata sets against ISO 15489 and 23081–1` including record keeping and archival metadata sets and schemas such as Dublin Core[9], ISAD/G EAD[10], ISAAR[11] and RKMS[12].

4.4.4 Additional standards and best practice guides for records management

In addition to the core documents above there is a wide range of guidance documents from The National Archives including the evaluation workbook to assist public authorities in assessing conformance of their records management systems to the Records Management Code issued by the Lord Chancellor (see Section 4.4.5 below). Other TNA guidance includes the following:

- File creation
- Tracking records
- Storage of semi-current records
- Business recovery plans

- Discontinued and transferred functions
- Documentation of records work
- Preparation of records for transfer to The National Archives
- Closure on transfer guidelines
- HR aspects of records management
- How to complete an information survey of records
- Management of records of temporary bodies
- Management of private office papers
- Management of audiovisual records
- Model retention and disposal schedules
- Cataloguing guidelines
- Access to public records guidance manual.

Other relevant standards and best practice guides for records management and archiving include the following:

Standards

Records storage	BS 5454:2000 Recommendations for the Storage and Exhibition of Archival Documents
Cataloguing	International Council on Archives, General International Standard of Archival Description [ISAD (G)], 2nd edition, 1999
Conservation and preservation	BS 4971:2002, Repair and allied processes for the conservation of documents – Recommendations BS 1153, Recommendations for processing and storage of silver-gelatine-type microfilm
Records management	BS ISO 15489-1:2001, Information and documentation – records management

4.4.5 Records management legislation and compliance issues in the public sector

The core piece of legislation for central government departments is the Public Records Act 1958 which places the responsibility on government departments and other organisations within the scope of the Act for making arrangements for selecting those of their records which ought to be permanently preserved and for keeping them in proper conditions. It further requires these arrangements to be carried out under the guidance of the Keeper of Public Records who is responsible for co-ordinating and supervising the work of selection.

Fig 4.7
The National Archives at Kew is responsible for the preservation of selected government documents

The Act lays down that documents selected for preservation shall be sent to the The National Archives (Fig. 4.7) not later than thirty years after their creation but that their transfer may, for administrative or other special reasons, be postponed with the Lord Chancellor's approval.

In the *Modernising Government White paper*[13] of 1999 all central government organisations were set a target to create and manage all new records electronically by 2004. Following on from the target, The National Archives continues to work with government departments, the wider public sector and other stakeholders to develop, implement and improve the standard of electronic records management across the public sector. The TNA Records Management Department was for some years the main point of contact between TNA and central government departments and agencies. To help accomplish this demanding task, TNA has recently set up a records management advisory service, now part of the National Advisory Services (NAS), the remit of which has been broadened to provide advice to the public sector.

In 2000, however, the Freedom of Information Act[14] introduced significant changes to the Public Records Act of January 2005. The Act replaced the access provisions for UK public records set out in the Public Records Acts 1958 and 1967 and governs access to information held by most public sector bodies.

The Lord Chancellor has issued two codes of practice under the Act. The section 45 code sets out good practice in handling requests for information. The section 46 code[15] is in two parts. Part I sets out good practice in records management and applies to all FOI authorities and also to bodies that are subject to the Public Records Act 1958 or the Public Records Act (Northern Ireland) Act 1923. Part II is aimed at records offices holding public records, and departments from which those records are transferred. It sets out how records should be transferred.

The National Archives has developed an evaluation workbook in the form of a consultation draft to assist public authorities in assessing conformance of their record management systems to the Records Management Code[16]. The National Archives has also produced or collaborated in the production of model action plans to help different parts of the public sector achieve compliance with the Records Management Code[17]. Most recently, TNA has developed a self-assessment programme and guide[18] designed to assist public bodies in carrying out internal audits to determine whether their records management systems comply with the Code.

The Data Protection Act[19] was passed in July 1998. The National Archives has produced a guide[20] setting out how the Act affects records managers and archivists.

The Freedom of Information Act gives rights of access to a wide range of information. However, rights of access to environmental information are provided by a separate statutory regime, the Environmental Information Regulations. New regulations were laid in December 2004[21] which bring into UK law a new EU directive 2003/4EC on public access to environmental information. The new regulations came into effect in January 2005 and replace the 1992 Environmental Information Regulations. Further information about access to environmental information, including guidance on the Regulations can be found on the website of Defra.

4.4.6 Requirements and best practice for electronic records management

Organisations should also review two key documents that are designed to help define requirements for ERM systems. They are the *Model Requirements for the Management of Electronic Records (MoReq)*[22] which was prepared for the IDA programme of the European Commission by Cornwell Affiliates plc and is now being revised, and the latest version of *The National Archives Requirements for Electronic Records Management Systems*[23].

The National Archives document clarifies the fact that 'these generic requirements are not a full specification. They form a baseline that sets out, in the mandatory part of the requirements, the minimum necessary to undertake credible electronic records management.' The TNA document was always designed to form part of a compliance scheme. Hence it contained a set of functional requirements that supplier products could be tested against and the TNA set up a testing programme in the UK.

The original MoReq document is similar to The National Archives document but there are three main differences. MoReq was designed to be equally applicable to the private and public sectors whereas The National Archives document was for UK government use specifically. Secondly, MoReq was designed to be international in scope and was translated into the languages of the European member states. Thirdly, the original MoReq document was not designed to form part of a compliance scheme.

Like The National Archives document, the MoReq document contains a generic set of functional requirements. It was intended to be used by potential ERMS users as a basis for preparing a

statement of requirements, by ERMS users as a basis for auditing or checking an existing ERMS, by training organisations as a reference document for preparing course material, and by ERMS suppliers and developers to guide product development.

National Archives 2002 Entities	MoReq 2001 Entities
Class	Class/Level
Electronic/Paper/Hybrid folder	Electronic/Physical file
Electronic/Paper/Hybrid folder part	Electronic/Physical volume
Electronic/Paper record	Electronic/Physical record
Electronic component	Electronic/Physical document copy
	Electronic/Physical document version

The key entities defined in each document are similar and are presented in the table above. Unfortunately, the terms used to describe them differ. The National Archives uses the term Electronic/Hybrid/Paper Folder whereas MoReq uses the term Electronic/Hybrid/Physical File. The National Archives avoids the word 'File' as this is used in computer systems to describe a lower level object such as a content file or a document file. Both mean the same – the old physical file folder or a new virtual electronic folder. The National Archives divides a folder into Parts, while MoReq prefers to use the term 'Volume'. The National Archives does not use the term 'Document' now – preferring 'Component' to cater for content objects as opposed to documents.

In 2005 TNA announced that the current phase of the evaluation scheme would complete at the end of 2005. The key dates were a cut-off for expressions of interest at the end of March 2005 and a deadline of end of June 2005 for fully worked submissions prior to testing. TNA will keep a list of approved products accessible and the requirements will be kept accessible for any public sector organisation to tailor and augment to meet their needs. Hence the TNA 2002 ERMS requirements are still a useful document to refer when developing ITTs.

From 2006, attention shifted to Europe where efforts were made by the EU Document Lifecycle Management (DLM) Forum to set up a new EU de facto standard (MoReq2) and an associated compliance testing regime with an appropriate organisation. At the DLM Forum in 2005 Ian Macfarlane of TNA reported on the plans for MoReq2. The scoping report for MoReq2 was endorsed and funding was agreed. As we went to press the contract was awarded to a consortium headed by Cornwell Management Consultants who authored the original document.

The overall aims for the MoReq2 development are to develop extended functional requirements within a European context and to support a compliance scheme by:

- Strengthening from MoReq what have become key areas and covering important new areas of requirements with clarity
- Ensuring that the functional requirements are testable and

MoReq base module

1. Introduction
2. Overview of ERMS requirements
3. Classification scheme
4. Controls and security
5. Retention and disposal
6. Capturing records
7. Referencing
8. Searching, retrieval and rendering
9. Administrative functions
10. Optional modules (see below)
11. Non functional requirements
12. Metadata requirements

Requirement Comparisons – National Archives versus MoReq

The 2002 National Archives document defines a series of ten core requirements followed by three optional requirements.

- **Record organisation**, which covers the classification scheme, classes, folders and folder parts. The equivalent MoReq section is the 'Classification scheme'.
- **Record capture, declaration and management**, which covers how records should be captured, declared as records and managed and covers record metadata, move, copy, extract and relate functions, and bulk import facilities. The equivalent MoReq section is 'Capturing records'.
- **Search, display and presentation**, which covers those functions. The equivalent MoReq section is 'Searching, retrieval and rendering'.
- **Retention and disposal**, is a major section covering disposal schedule definition, allocation and execution, resolving conflicts, review and destruction. The MoReq section has the same title.
- **Access control**, covers access to ERMS, access control markings, roles, groups, allocation to classes folders and records, custodian, execution of access control markings and privacy and opening of records. The equivalent MoReq section is part of 'Controls and security'.
- **Audit**, defines the audit trail requirements. The MoReq equivalent is in 'Controls and security'.
- **Reporting**, defines all the reporting requirements. MoReq covers this under 'Administrative functions'.
- **Usability**, defines the user interface requirements. MoReq covers this under 'Non-functional requirements'.
- **Design and performance**, covers integrity, interfaces, disaster recovery, storage, performance and scalability. MoReq covers this under 'Non-functional requirements'.
- **Compliance** with other standards. MoReq covers this in its Annexes.

The National Archives document includes three optional modules. These are not a mandatory part of the core ERM requirements. However, if an ERMS supplier wishes to demonstrate a capability of providing one or more of the functions covered by the optional modules, within the context of ERM, then the system must fulfill all of the mandatory requirements in that module.

- **Authentication and encryption**, covers electronic signatures, electronic watermarks ands encryption.
- **Document management**, covers high-level requirements for an integrated EDRM system but does not include a detailed EDM specification.
- **Hybrid and physical folder management**, covers additional requirements for systems that will be required to manage both paper and electronic folders. It covers physical folders, markers, retrieval and access control and tracking and circulation and disposal.

For many users the document management and hybrid requirements will be mandatory so they should be studied carefully. The equivalent requirements are covered by MoReq in 'Other functionality'. The latest National Archives document promises other optional modules in future, which will cover content management, casework and workflow, image management and document scanning and preparing records for transfer.

developing test materials to enable products to be tested for compliance with the requirements
- Making the requirements modular to assist application in the various environments in which they will be used.

To provide compatibility, MoReq2 is to be an evolutionary update to the original MoReq, not a radically different product.

The MoReq requirements are to be arranged in a base module which constitutes the minimum necessary to provide credible electronic records management and as optional modules. The base includes sections 1–9, 11 and 12 the metadata requirements.

The proposed arrangement of optional modules (a modified section 10) is as follows:

MoReq optional modules

- Management of physical records and hybrid file retention and disposal (existing)
- Document management and collaborative working (existing)
- Integration with workflow (existing)
- Casework (new)
- Integration with content management systems (new)
- Electronic signatures, encryption, electronic watermarking (existing)
- Distributed systems (new, including existing requirements drawn from base and other sections)
- Offline and remote working (new)
- Definition and description of record keeping processes (new)
- Fax integration (new)
- Security categories (from 4.6).

So, at present, the TNA requirements are the standard to follow. In future this role will pass to MoReq2 which is due to be published at the end of 2007. In 2008 we should see the start of a new testing programme that will run across Europe.

TNA has also produced the *e-Government Policy/Framework for Electronic Records Management*[24] with the eGovernment Unit in 2001 and a set of background guidelines on the management, appraisal and preservation of electronic records.

The National Archives has also produced a set of toolkits to help organisations develop electronic document and records management, including:
- How to produce a corporate policy on electronic records
- Toolkit for compiling an inventory of electronic records
- Toolkit for appraising the inventory of electronic records
- Good practice in managing electronic documents using Office 97 on a local area network
- Framework for strategic planning and implementation
- Sustainable electronic records, strategies for the maintenance and preservation management of electronic records on websites and intranets, and an ERM toolkit
- Business classification scheme design
- Guidelines on developing a policy for managing e-mail
- Guidance publication on realising benefits.

4.4.7 Requirements and best practice for electronic records preservation and archiving

When the TNA ERMS requirements were first produced in 1999 they were aimed at government departments, and the traditional model was that they would manage their own records while they were active and semi-active. They would then review them and the TNA would be invited to select a small percentage deemed worthy of long-term preservation. This placed the onus for the long-term preservation of government records on The National Archives and they have gone on to develop their own electronic archive as described below. Hence the initial requirements did not cover the issue of long-term preservation of electronic records in detail.

However, it was soon recognised that government departments also would need to manage electronic records that were not required by The National Archives but which nevertheless had to be kept accessible for long periods. Outside of central government many public sector bodies will have to manage records in electronic format for long periods of time.

Fortunately there are a growing number of sources of expertise and guidance on the archiving and preservation of electronic data and records.

The National Archives has produced two relevant documents
- The Management, Appraisal and Preservation of Electronic Records, Vol.1 Principles, Vol.2 Procedures (see box below).
- The National Archives, The Generic Requirements for Sustaining Electronic Information over Time (2003)

Jones and Beagrie also produced an excellent work *Preservation management of digital materials: a handbook*[25].

The Management, Appraisal and Preservation of Electronic Records

Volume 1	Records management in information age government
	Electronic records in the organisation
	Record organisation and structure
	Management of electronic records
	Design of electronic records management systems
	Strategies for developing electronic records management
Volume 2	Creating and capturing records
	Managing and maintaining records
	Inventory, appraisal and disposal
	Preservation of electronic records
	Safeguarding records from Year 2000
	Outline functional requirements
	Relevant standards

The scoping report for MoReq2 confirmed that metadata elements of preservation will be included. It will be ensured that the metadata is compatible with ISO 23081 (Principles for metadata) and with the OAIS (Open Archival Information System standard ISO 14721). ISO 23081 is reviewed above. The OAIS standard is reviewed below.

ISO 14721:2003[26] specifies a reference model for an open archival information system (OAIS). The purpose is to establish a system for archiving information both digitised and physical with an organisational scheme composed of people who accept the responsibility to preserve information and make it available to a designated community. This reference model addresses a full range of archival information preservation functions including ingest, archival storage, data management, access and dissemination. It also addresses the migration of digital information to new media and forms, the data models used to represent the information, the role of software in information preservation and the exchange of digital information among archives. It identifies both internal and external interfaces to the archive functions and it identifies a number of high level services at these interfaces. It provides various illustrative examples and some best practice recommendations. It defines a minimal set of responsibilities for an archive to be called an OAIS and it also defines a maximal archive to provide a broad set of useful terms and concepts.

The National Archives have set up their electronic archive to comply with this model. Such a solution needs a hierarchical digital storage solution. The National Archives used FileTek's StorHouse which is built around products such as EMC's Centera and MAID. You also need application software, and The National Archives used Tessella Support Services to develop the application.

The US's National Archives and Records Agency (NARA) has also recently let a $300 million contract to Lockheed Martin to develop an Electronic Records Archive which employs similar software.

The Digital Preservation Coalition (www.dpconline.org) is a useful source of information on all aspects of digital preservation. It is supported by JISC, the British Library and others. They have published *Directory of Digital Preservation Repositories and Services in the UK*. This includes a listing of archive data services.

Other information sources are the Digital Curation Centre funded by JISC (www.dcc.ac.uk) and ERPANET the Electronic Resources Preservation and Access Network (www.erpanet.org).

Another relevant standard is METS[27] (Metadata Encoding and Transmission Standard) which is maintained by the US Library of Congress. For a major archive project – Making of America II (MOA) – the Library provided an encoding format for descriptive, administrative and structural metadata for textual and image-based works. METS, a Digital Library Federation initiative, attempts to build upon the work of MOA and provide an XML document format for encoding metadata necessary for both management of the digital library objects within a repository and exchange of such objects between repositories (or between repositories and their users). Depending on its use a METS document could be used in the role of Submission Information Package (SIP), Archival Information Package (AIP) or Dissemination Information Package (DIP) within the Open Archive Information System (OAIS) reference model so it is tightly linked to the OAIS standard referenced above. A METS document consists of seven major sections – METS header, descriptive metadata, administrative metadata, file section, structural map, structural links and behaviour.

One of the issues when archiving electronic records is whether you hold them in an editable, viewable and printable or read-only form. Where archives need to hold records in an editable form one of the key standards is the Open Document Format being developed by OASIS. For the read-only static format the new PDF Archive format (ISO 19005-1:2005) would be appropriate.

OASIS[28] is the Organisation for the Advancement of Structured Information Standards. It is a not-for-profit international consortium that drives the development, convergence and adoption of e-business standards. The consortium produces more web services standards than any other organisation along with standards for security, e-business and standardisation efforts in the public sector. Founded in 1993 OASIS has more than 5,000 participants representing over 600 organisations. The consortium hosts two of the most widely respected portals on XML and web services standards. OASIS was originally founded under the name SGML Open as a consortium of vendors and users devoted to developing guidelines for interoperability among products that supported the standard generalised markup language (SGML). OASIS changed its name in 1998 to reflect an expanded scope of technical work including the extensible markup language (XML) and other related standards.

ISO 19005–1:2005 *Document management – Electronic document file format for long-term preservation – Part 1: Use of PDF 1.4 (PDF/A-1)*[29]. PDF/A is a constrained form of Adobe PDF version 1.4 intended to be suitable for long-term preservation of page-oriented documents for which PDF is already being used in practice. The standard was developed by an ISO working group with representatives from government, industry and academia and active support from Adobe. PDF/A attempts to maximise device independence, self containment and self documentation.

References:

1. *Information as an asset: the board agenda*. A consultative document by the Hawley Committee. 16pp. 1995. Dr Nigel Horne, KPMG IMPACT Programme.
2. ISO 15489:2001 *Information and documentation – Records management*. BSI Business Information, 389 Chiswick High Road, London W4 4AL, www.bsi-global.com.
3. BSI BIP 0008:2004 *Code of practice for legal admissibility and evidential weight of information stored electronically*. BSI Business Information, 389 Chiswick High Road, London W4 4AL, www.bsi-global.com.
4. National Archives. *Management, appraisal and preservation of electronic records*. Vol. 1 Principles and Vol. 2 Procedures. www.nationalarchives.gov.uk/recordsmanagement.
5. JISC. *Implementing an Electronic Document and Records Management (EDRM) System*. JISC applied infoKit. www.jiscinfonet.ac.uk.
6. BSI DISC PD0010 *Principles of Good Practice for Information Management*. Bill Mayon White and Bernard Dyer. BSI Business Information, 389 Chiswick High Road, London W4 4AL, www.bsi-global.com.
7. BSI EN ISO 9000 *Quality management and quality assurance standards*. BSI Customer Services. www.bsi-global.com.
8. ISO 23081–1 Information and documentation – Records management processes – metadata for records – Part 1 – Principles. Reference number ISO 23081-1:2006(E). ISO 2006. ISO copyright office, Case postale 56, CH-1211 Geneva 20. Tel + 41 22 749 01 11 E-mail copyright@iso.org. www.iso.org.
9. www.dublincore.org
10. ISAD/G EAD. www.ica.org.
11. ISAAR. www.ica.org.
12. RKMS. www.ifla.org/documents/libraries/cataloguing/rkms_pt1&2pdf.
13. *Modernising Government*. White Paper. www.archive.official-documents.co.uk/document/cm43/4310/4310.htm
14. *Freedom of Information Act 2000*. www.opsi.gov.uk/acts/acts2000/20000036.htm.
15. Lord Chancellor's *Code of practice on the management of records under section 46 of the Freedom of Information Act 2000*. www.dca.gov.uk/foi/reference/imprep/codemanrec.htm.
16. *Complying with the Records Management Code: evaluation workbook and methodology – consultation draft*. www.nationalarchives.gov.uk/recordsmanagement/code/assessing.htm.
17. www.nationalarchives.gov.uk/policy/foi.
18. *Section 46: Information management assessment programme*. www.nationalarchives.gov.uk/recordsmanagement/code/section46.htm.
19. *Data Protection Act 1998*. www.opsi.gov.uk/acts/acts1998/19980029.htm
20. www.nationalarchives.gov.uk/policy/dp.
21. *Statutory Instruments 2004: No. 3391*. The Environmental Information Regulations 2004 www.ico.gov.uk.
22. *Model Requirements for the Management of Electronic Records (MoReq)*. CECA-CEE-CEEA, 2001. http://ec.europa.eu/idabc/en/document/2303/5644.
23. National Archives. *Requirements for Electronic Records Management Systems*. 2002 revision. www.nationalarchives.gov.uk.
24. *e-Government Policy Framework for Electronic Records Management*. www.nationalarchives.gov.uk/electronicrecords/.
25. Jones, M. and Beagrie, N. *Preservation management of digital materials: a handbook*. Resource and the British Library 2001.
26. ISO 14721:2003. Space data and information transfer systems – Open archival information system – Reference model. www.iso.ch.
27. METS. www.loc.gov/standards/mets/METSOverview.v2.html.
28. OASIS. www.oasis-open.org.
29. ISO 19005–1:2005 *Document management – Electronic document file format for long-term preservation – Part 1: Use of PDF 1.4 (PDF/A-1)*. www.iso.ch.