Managing Information and Records

The definitive guide—2013 Edition

Sponsored by C-Cube Solutions

Chapter 2

Improving Corporate Information and Records Management

● Information and Records Management Best Practice ● IRM Solution Options ● Enterprise Content Management from A to Z ● Designing and Implementing an IRM Solution ● Making the Business Case

Cimtech
Innovation Centre ● University of Hertfordshire ● College Lane ● Hatfield ● Herts ● AL10 9AB ● www.cimtech.co.uk

information OVERLOAD

Do you want to spend time searching or finding

Do you want compliance

Do you want process efficiencies

?

OITUK Ltd., specializes in providing C-Cube Electronic Document and Content Management & Workflow solutions, based on the C-Cube software suite. Systems scale from small departmental applications to large enterprise -wide solutions and include: the C-Cube Portal, Electronic Forms, Content Searching, and C-Cube Electronic Document & Records Management System (EDRMS), offering specialised solutions, including:

- Legal Compliance
- Health Records Management
- Law Enforcement Applications
- Information Web Portals
- Invoice Capture and Authorisation
- Local Authority Applications
- Human Resource Management

The key to all C-Cube Solutions is integration with your business to ensure that information is delivered on time and to the right place. C-Cube Solutions have met customer requirements in the public and private sectors over the last 15 years using the following underlying technologies:

- Document Management
- Workflow
- Web Portal & XML Integration
- COLD / Microfiche Integration
- Electronic Forms Processing
- Electronic Records Management
- Collaboration Facilities

DM DOCUMENT MANAGER AWARDS 2010 WINNER Project of the year - Public Sector CCubesolutions from OITUK Ltd St Helens & Knowsley NHS Trust

DM DOCUMENT MANAGER AWARDS 2010 RUNNER-UP Document Manager Product of the Year CCubesolutions from OITUK Ltd C-Cube Portal

the information people

ccube solutions

CCube Solutions
13 Diamond Court
Opal Drive,
Fox Milne
Milton Keynes,
MK15 0DU

Call:	+44 (0)1908 677 752
Email:	sales@ccubesolutions.com
Web:	ccubesolutions.com

CCube Solutions is a trading name of OITUK Ltd.
Registered in England & Wales, No: 04727067

CONTENTS

Chapter 2

Improving Corporate Information And Records Management: a guide to best practice

2.1 Coverage

In this chapter we show why you need good information and records management and how to set about making improvements. Section 2.2 makes the case for improving corporate information and records management. Sections 2.3 and 2.4 help you set up a framework of policies and procedures and roles and responsibilities and section 2.5 points you towards standards and best practice.

2.2 The Case for Improved Information and Records Management

2.2.1 What is Information?

Figure 2.1 shows the traditional hierarchical diagram. At the bottom is raw data. Above that is information which can be thought of as data that is organised, put in context and given meaning. The ability to find the right information at the right time is vital to any organisation and some have invested £millions in computer systems which help them achieve just that. Above that is knowledge, which is information understood and acquired. Knowledge Management is a set of strategies and technologies that assist with the acquisition processes. Finally, at the top of the pyramid is wisdom which is knowledge that is applied and exploited.

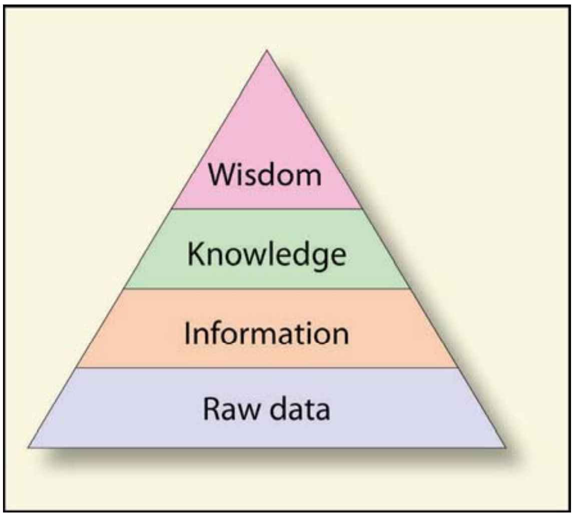


Fig.2.1
The information hierarchy

For all organisations, the information they possess is one of the four core strategic assets, alongside finance, staff and property. Without it they would be unable to operate. Many organisations do not fully understand the value of the information assets they hold and are not using them to their full potential. In many cases they are not even protecting them, leaving them vulnerable to loss or theft.

Organisations hold their corporate information in databases, documents and a variety of media and formats. We often refer to data in databases as structured information and information in documents and other objects as unstructured information. Structured information is usually well managed in databases but still presents challenges when it comes to retention, disposal and digital preservation. Unstructured information is more diverse and harder to control. It includes text, graphics, images, audio and video content. It may be held online in digital format or offline on tapes, CDs and USB sticks or on paper or other analogue media.

Particular issues arise with emails. Emails are not usually integrated with other sources of information, increasing the barriers to finding the right information at the right time. Other electronic documents may be dispersed between shared drives, document management systems, intranets, internets and externally hosted systems. Increasingly, employees are storing corporate information on social networking sites outside the control of the organisation that they work for. New collaboration methods speed up conversations and decisions but often make it harder for organisations to find and manage their information in the longer term.

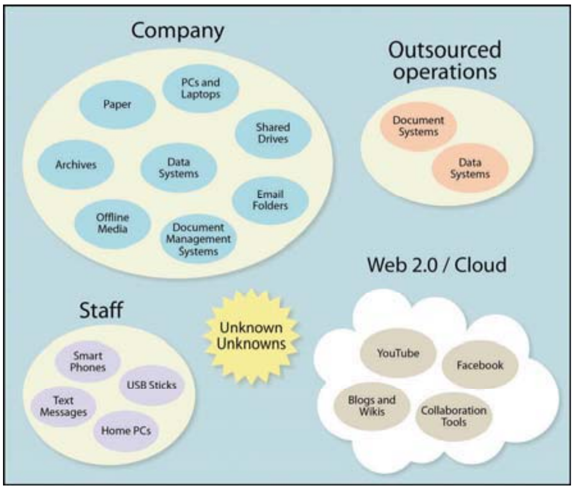
Information may be divided into categories such as reference, administrative, open or restricted, transient or permanent. It is not all of equal value. The value of information varies and the length of time it needs to be kept varies but it all needs to be managed, whether to ensure early deletion or to enable long-term preservation.

A subset of all the information held by organisations can be considered as records, indicating that they need to be retained, whether for legal, operational or other reasons. The records management standard ISO 15489-1:2001 defines records as 'information created, received, and maintained as evidence and information by an organization or person, in pursuance of legal obligations or in the transaction of business'. However, it should be remembered that UK and EU legislation makes no distinction between records and other information and even the most seemingly trivial email or text message might become crucial evidence in court.

A smaller subset of records can be categorised as vital records, those without which the organisation cannot operate. These vital records should be identified and protected and made easily accessible to authorised users but, again, the fact that they may be held on paper or in digital format on a range of applications and in a vast array of formats makes it very difficult for organisations to identify and manage all their vital records effectively.

Figure 2.2 gives a simplified view of where your corporate information may be located. In reality there are many more locations and new options springing up all the time, hence the 'unknown unknowns'.

Fig.2.2
Where is your corporate information?



2.2.2 What is Information Management?

Information management is a generic term used to cover a wide range of disciplines, professions and software solutions which together are designed to help us keep our information under control, accessible and managed like any other corporate asset.

Records management as a discipline traditionally focussed on managing paper but now with much wider responsibility includes all forms of digital information and indeed data applications. Records managers carry out a range of activities such as auditing information, creating classification schemes for shared drives or document management systems, creating and applying retention and disposal schedules, managing physical storage and perhaps archives, enforcing filenaming and version control, planning digital preservation and implementing and managing Electronic Document and Records Management (EDRM) systems.

Information assurance and **information security** are increasingly important aspects of information management as the government tries to stem the leaks and losses, particularly of personal information, that continually hit the headlines. Information security as a discipline focuses on tools and technologies for protecting information, whereas information assurance is a wider field covering strategy, risk and behaviour as well as technologies.

Information Governance covers records management and information assurance and usually also includes the handling of requests for information. Under Data Protection legislation organisations must respond to requests by subjects for access to information about themselves. In the public sector the Freedom of Information Act requires organisations to respond to requests from the public for any information and the handling of such requests in a large organisation may occupy a whole team of staff.

Knowledge Management is about publishing and exploiting information through intranets and search engines and improved practices for collaboration and sharing. In central government this is reflected in the term KIM (Knowledge and Information Management) often used for the central information management team, but few organisations have a dedicated knowledge management role, most preferring to bring in specialist external consultancy.

2.2.3 Why is Information Management needed?

One very important reason for managing information well is to comply with information legislation. We also need to keep records in order to demonstrate compliance with a range of other legislation. Legislation includes:

- Data Protection Act 1998
- Privacy and Electronic Communications Regulations 2003
- Copyright, Designs and Patents Act 1988
- Health and Safety Acts (various)

Also important are:

- audit and accountability requirements
- legal admissibility

Many industries such as financial services, pharmaceuticals, construction industry, aviation and energy also have tough regulations requiring good record keeping.

In the public sector organisations have additional legislation to comply with:

- Freedom of Information Act 2000
- Environmental Information Regulations 2004
- Regulations on the Reuse of Public Sector Information 2005
- Public Records Acts 1958 and 1967 (central government only)
- Regulation of Investigatory Powers Act 2000
- Protection of Freedoms Act 2012

Government organisations should also comply with information security requirements e.g.:

- HMG Security Policy Framework v8 2012
- Local Public Services Data Handling Guidelines v2 2012

One important reason for record keeping in central government is the need to keep records for transfer to the National Archives. This is happening earlier now. The '30 year rule' which was the maximum time that central government departments could hold records without opening them to the public (subject to exemptions) has been reduced by the 2010 Constitutional Reforn and Governance Act to 20 years, with a phasing-in period.

2.2.4 What are the other benefits?

As well as making organisations compliant with legislation, good information management makes organisations more efficient and effective. It is no coincidence that the best brands and most respected organisations have the best information management.

Benefits can be divided into categories of financial, competitive and flexibility benefits. Financial benefits are mostly about reducing costs:

- staff costs
- space costs
- IT costs
- telephone costs
- travel costs
- contract management costs
- e-discovery costs
- lost claims and court cases

Competitive benefits help the organisation gain a greater share of the market:

- faster product development and reduced time to market
- lower sales costs
- improved customer service
- improved web sites
- more effective and focused marketing (business intelligence)
- improved customer image/brand reputation
- compliance with public sector/industry targets

Flexibility benefits help the organisation innovate and survive change:

- greater corporate agility
- faster introduction of new products and services
- improved staff management and development
- improved customer service/choice
- business continuity

Business continuity is an important and often overlooked benefit of information management. Good information management helps an organisation survive not only IT failures and physical disasters but also staff movement, absence and illness, mergers and acquisitions and other potentially disruptive events in its corporate history.

Chapter 6 explores the benefits further in 'Making the business case'.

2.2.5 How is information management improved?

Broadly speaking most organisations need to:

1. Issue policies and procedures;
2. Set up roles and responsibilities;
3. Undertake a programme of activity to bring the organisation's information management in line with its policies and procedures.

The International Standard *15489:2001 Information and documentation—Records Management*[1] covered in section 2.5 below sets out an 8-step programme of activity towards good records management.

First you will need an Information Management Policy (refer to Fig. 2.3 overleaf). But it is not sufficient to write an Information Management Policy: it must also be implemented throughout the organisation.

A full methodology for managing an information and records management project is provided in Chapter 5.

2.3 Policies and procedures

A good information management policy should be short and concise with implementation details left to subsequent procedure documents. Separate policies may be written for information and records management but there will be considerable overlap and a single information management policy can usually cover both.

A good IM policy document should include sections for: (Fig. 2.3 overleaf).

Policy statements

The following policy statements were published by the Cabinet Office in 2011[2] for the public sector but can be adapted for all organisations. The exposition in italics are Cimtech's:

1. Information is a valued asset
   Information assets will be identified and their value assessed.
2. Information is managed
   Information assets will be stored, managed, protected, preserved and exploited in a manner commensurate with their value and compliance requirements.

Fig.2.3 *Sections for an Information Management Policy*

Section	Content
Scope	This section states which business areas and information types are covered by the policy. The scope should include paper and electronic records and databases and social media.
Compliance	This section should list the legislation and corporate strategy applicable to the organisation's information management.
Policy statements	This section makes a corporate commitment to a list of policy statements. (see box below)
Roles and responsibilities	This section identifies central and local responsibilities and makes clear the responsibility of every member of staff for the information in their case. (see section below)
Approved storage	This section, without going into details, states how current and new systems and storage options will be approved for use.
Retention and disposal	This section states that retention schedules will be maintained and applied to all information.
Security	This commits the organisation to protecting its information and may refer to a separate Information Security or Assurance policy.
Implementation	This section commits the organisation to a programme of improvement where needed to comply with the policy.
Consultation	This section lists the stakeholders consulted and states which board or group approves the policy.
Monitoring	How compliance with the policy will be monitored and audited
Policy review	How and when the policy will be reviewed and who by.

3. Information is fit for purpose
   Information quality will be appropriate to its purpose. Information quality requires accuracy, validity, reliability, timeliness, relevance, and completeness.
4. Information is standardised and linkable
   Information will follow open standards and corporate standards and use common references that enable items to be linked, integrated, exchanged and migrated as necessary.
5. Information is re-used
   The potential for internal and external re-use will be assessed and mechanisms established.
6. Public information is published
   A framework will be established for responding to public access requests and for making public other information relevant and suitable for publication.

Strategy

After the policy is approved, the organisation will need a strategy for implementing the policy and improving records management. This might include the implementation of an Electronic Document and Records Management system or a plan to improve records management using existing desktop tools and server applications.

Procedures

Every organisation will need a set of guidance documents to help staff comply with the policy. These should include guidance on acceptable use of IT, email usage, home and mobile working, retention and disposal, managing paper files, handling personal information, information sharing and in some organisations protective marking . Guidance can be more effective if collated into documents directed towards a particular audience e.g. a guide for Information Asset Owners, another for Local Information Managers (see Roles and Responsibilities below) and one for all staff.

Section 1 of ISO 15489 contains a useful description of eleven recommended records management processes that can be used as a model for in-house procedures.

2.4 Roles and responsibilities

Roles and responsibilities are essential to an effective information governance framework. First a corporate Information Governance Group or board is needed to monitor the organisation's information management and initiate and fund projects. Then a central Information Governance team is needed to deliver policies, procedures, strategy and corporate projects. In all but the smallest organisations the records manager does not have time to get involved in detailed records management in all departments and needs the help of nominated Local Information Managers in each business unit.

The central team might include:

- An Information Governance Manager to oversee records management, information security/assurance and access to information.
- A Records Manager or to implement policies and procedures with retention schedules and classifications schemes, guidance and training and to manage central and offsite paper storage.
- An Information Security/Assurance Officer to implement technology solutions and ensure wider information assurance.
- Information Access Officers to handle Data Protection information access requests and in the public sector Freedom of Information access requests.

Often the team will sit in the Legal department or report to the Head of Compliance but some members may sit in the IT department. Either way close links with both IT and with Legal and Compliance departments are essential.

Key components of a successful information and records management

- 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 of 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.

Some useful roles have also emerged from the HMG Security Policy Framework. At the top is the Senior Information Risk Owner, a board-level officer who is accountable for the organisation's information risks. Then we have Information Asset Owners (IAOs) who are the heads of a service or unit and as well as being responsible for staff, performance and budgets are now held accountable for the information in their unit. IAOs will have line management control over Local Information Managers, which is useful for enforcement because records managers only have 'dotted line' control, i.e. guidance and monitoring, over the business.

If we merge the security roles with records management roles we have a recommended structure as below:

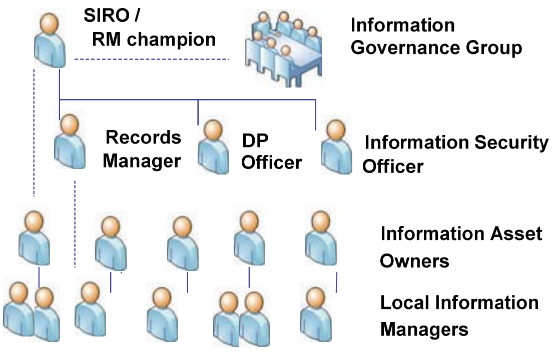


Fig.2.4
Recommended structure

In addition to the above roles we might need a trainer to help the records manager roll out training to all departments and external consultants such as Cimtech to provide special expertise or additional resources. Organisations undertaking a major information and records management involving the introduction of EDRM will also need an experienced project manager.

A full methodology for managing an information and records management project is provided in Chapter 5.

2.5 Best Practice for Information and Records Management

One of the key tasks to be carried out by an organisation is to benchmark current corporate information and records management policies, procedures and systems against best practice guidelines and standards.

There are a number of published guides and standards for best practice in information and records management.

2.5.1 Principles of good practice

More than 15 years old now, but still relevant, are the *BSI DISC PD0010*[3] *Principles of Good Practice for Information Management* by Bill Mayon White and Bernard Dyer with input from many other organisations (Fig. 2.5).

There are five main principles which take the form of a set of statements of objectives for information management, to be taken forward into new methods and technologies for managing information:

- 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.

2.5.2 ISO 15489-1:2001 Information and documentation-records management

ISO 15489:2001 Information and documentation-records management[1] is an international standard derived from the Australian Standard AS 4390. The standard provides a framework and pro-

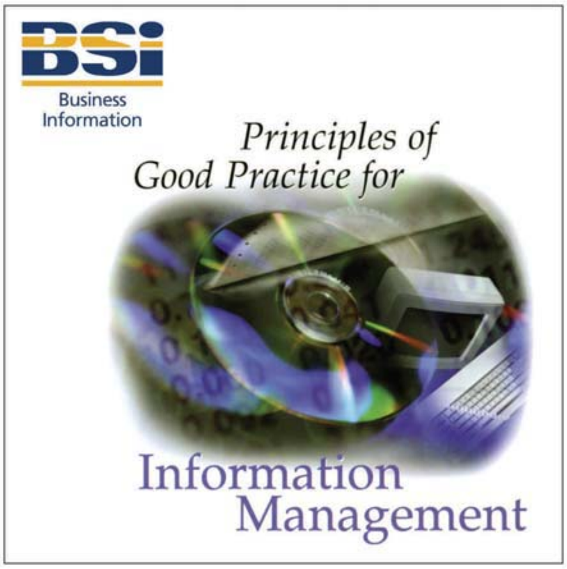


Fig.2.5
A number of published guides are available covering best practice

gramme for organisations establishing a records management system.

Part 1 of ISO 15489 provides general guidance to managers on establishing records management policies, procedures and systems. It defines a comprehensive records programme, which includes determining what records should be created in each business process 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 the adoption of a records management strategy that 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 a guide for use by records management professionals in implementing Part 1. It includes an eight-point plan for designing and implementing a records system based on the Australian DIRKS (Designing and Implementing Recordkeeping Systems) methodology.

Note that it does not offer a set of requirements for a records management system, for which we look to standards from The National Archives and MoReq (section 2.5.7 refers).

2.5.3 ISO 30300 series

Whereas ISO 15489 sets out a framework and programme of activity towards good records management, the complementary ISO 30300:2011[4] series provides a management system and measurement method for records management equivalent in method to the quality management system ISO 9000, the environmental management system ISO 14000 and the information security management system ISO 27000. Like the other management systems ISO 30300 is a method of controlling processes, auditing them against a set of standard controls and ensuring continuous improvement through annual review.

So far in early 2013 we have:

- *ISO 30300—Management Systems for Records—Fundamentals and Vocabulary.*
- *ISO 30301—Management Systems for Records—Requirements.*

To follow are three more publications that will enable audit and certification against the standard:

- *ISO 30302—Management Systems for Records—Implementation Guide.*
- *ISO 30303—Management Systems for Records—Requirements for bodies providing audit and certification.*
- *ISO 30304—Management Systems for Records—Assessment Guide.*

2.5.4 Information Security and Assurance

To help organisations manage information security we have the *ISO 27001 International Standard for Information Security 2005*[5] which is the standard for a management system that goes beyond security technology to cover a wide range of sources of information risk. The standard defines 133 controls under 11 objectives:

- Information security policy
- Organising information security
- Asset management
- Human resources security
- Physical and environmental security
- Communications and operations management
- Access control
- Information systems acquisition, development and management
- Information security incident management
- Business continuity management
- Compliance

ISO 27001 can be cut down to suit a smaller organisation but remains a difficult standard to achieve. If corporate certification is not within reach for your organisation the individual requirements are each worth studying and implementing as far as possible through procedures and technologies.

For more achievable information security the 2008 *Data Handling Procedures in Government*[6] provide basic rules for data protection and information assurance. For central government there is the 2012 *HMG Security Policy Framework* v8 and for local government the *2012 Local Public Services Data Handling Guidelines* v2. All of these require the creation of an Information Asset Register i.e. a list of all the information assets that an organisation holds, along with their attributes such as owner department, purpose, type of information and handling requirements.

There is also much useful guidance about handling personal data on the Information Commissioner's Office website www.ico.gov.uk.

2.5.5 Legal admissibility

To ensure that your digital documents can be confidently used in court, the British standard *BS 10008:2008 Evidential weight and legal admissibility of electronic information. Specification and the related BIP 0008:2008 Code of Practice*[7] offer useful advice on the systems and scanning procedures necessary to ensure data quality and auditability.

Organisations which conduct large volumes of scanning or have a service to offer are recommended to seek certification of compliance with the BS 10008 standard. Other organisations would do well to follow the standard and use it as a checklist to see what improvements need to be made.

2.5.6 Public sector requirements

In the public sector the main legal requirement for records management is laid down in section 46 of the Freedom of Information Act 2000. For central government there is the additional need to preserve records, appraise them and transfer selected records to The National Archives and other places of deposit, which is laid down in the Public Records Acts of 1958 and 1967 with the timing amended in the 2010 Constitutional Reforrn and Governance Act.

To assist with public sector legal requirements the National Archives drew up the *Lord Chancellor's Code of Practice* revised in 2009[8] and commonly known as the 'RM Code'.

Part 1 sets out requirements for all public sector bodies under headings of:

1. Organisational arrangements to support records management
2. Records management policy
3. Keeping records to meet corporate requirements
4. Records systems
5. Storage and maintenance of records
6. Security and access
7. Disposal of records
8. Records created in the course of collaborative working or through out-sourcing
9. Monitoring and reporting on records management

Part 2 is specifically for central government to enable the maintenance, review and transfer of public records to the TNA and other archives.

The TNA has developed a self-assessment programme to assist public bodies in carrying out internal audits to determine whether their records management systems comply with the RM Code. It has issued a self-assessment questionnaire[9] to enable organisations to measure their compliance with the Code.

2.5.7 Electronic records management

Organisations seeking to implement EDRM or other forms of electronic records management solution are advised to follow standards not only in order to implement best practice but also to enable interoperability between systems and make possible the migration of content (plus metadata, audit trails and other attributes) to future EDRM systems.

TNA 'Requirements for Electronic Records Management Systems'

The first standard set of functional requirements for the UK public sector was produced by The National Archives in 1999 and was called *Requirements for Electronic Records Management Systems*. It was revised in 2002 to include a metadata standard. The TNA:2002 *Requirements for ERMS*[10] were accompanied by a compliance scheme. A testing programme in the UK awarded compliance to approximately 20 products at different times before the scheme was withdrawn in 2005 in favour of support for MoReq (see below).

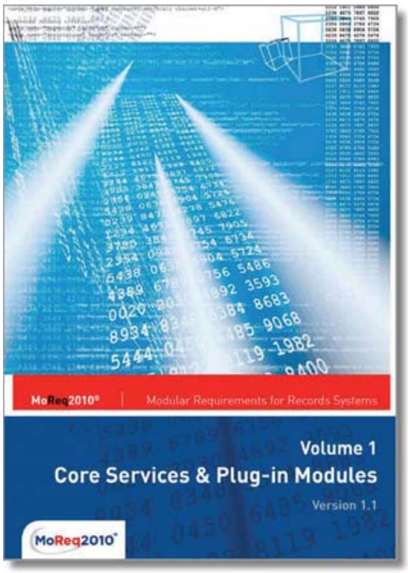
Although the *Requirements for ERMS* are no longer recommended for use in EDRM procurement, at the time of writing they provide the only accreditation that products can demonstrate. A product that has in the past been accredited by the TNA shows evidence of a comprehensive set of records management functionality and supplier commitment to standards. Hence the TNA:2002 *Requirements for ERMS* is still a useful checklist when developing a statement of requirements but buyers can no longer ask for contractual compliance.

MoReq

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.

The original *Model Requirements for the Management of Electronic Records* (MoReq) was issued in 2001 as a set of functional requirements which unlike TNA:2002 had EU-wide applicability in both public and private sectors. The second version MoReq2, issued in 2008, instigated a testing regime but by the end of testing only one product was accredited. In 2010 The DLM Forum commis-

Fig.2.6 MoReq2010 was published in 2011


MoReq2010® | Modular Requirements for Records Systems
Volume 1
Core Services & Plug-in Modules
Version 1.1
MoReq2010®

sioned a third version which was a radical redesign known as MoReq2010[11] and published in 2011.

MoReq2010 makes several useful changes. Now entitled *'Modular Requirements for Records Systems'* the new specification takes a modular approach which enables products to achieve compliance on a module by module basis. Some of the MoReq2010 -compliant records systems (MCRSs) might not look like records management systems but might in fact be finance systems or email systems that include compliant functionality for the records they contain. Under MoReq2010 not only must products be compliant but also individual implementations. This plugs a gap now evident in the TNA accreditation scheme in which a compliant system could be configured out of compliance during implementation, making interoperability and future migration more problematic than it should have been.

At the time of writing (early 2013) two vendors have committed products to MoReq2010 testing but no results have been published.

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 record collections
- 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

2.5.8 Metadata standards

ISO 15489 defines metadata as 'data describing the context, content and structure of records and their management through time'. If you are implementing an EDRM system or similar system that provides metadata fields to augment your content you will want to follow best practice and common standards.

Following best practice will improve your ability to search and administer the system. Common standards will assist with interoperability between different systems and migration to successive systems over time.

We have a number of standards relating to metadata.

***ISO 23081-1:2006 Information and documentation—Records management processes—Metadata for records*[12]**

ISO 23081 does not actually offer a list of standard metadata but helps with the evaluation of standards.

Part 1:2006 sets a framework for creating, managing and using records management metadata and explains the principles that govern them. Part 2:2009 is more explanatory and provides practical guidance on implementation issues and how to assess records management metadata sets against the principles. Part 3:2011 provides an assessment of existing metadata sets against ISO 15489 and 23081-1.

***ISO 15836:2009 Information and documentation-The Dublin Core metadata element set*[13]**

Unlike ISO 23081, ISO 15836 does set metadata standards and the standards it sets are based on the Dublin Core Metadata Element Set, which was established in 1995 and remains the most widely known and most widely used set of metadata. ISO 15836 metadata elements are useful for discovery, for example in publishing systems such as web sites, but are usually supplemented with other metadata to cover attributes for records management.

E-Government Metadata Standards

In 2006 the UK created a standard set of metadata for government in the e-Government Metadata Standard (e-GMS V3.1)[14]. This set of metadata aligned with the TNA:2002 metadata and has not been superseded by any new standard but is no longer promoted.

For an organisation starting to implement EDRM at the current time and trying to select a metadata standard we must decide between the incomplete ISO 15836, the apparently defunct e-GMS and the as yet unadopted MoReq2010, but can take heart in noting that there is a great deal of commonality among the three.

Specialist metadata standards

If your information is of a specific type (geographic, images, scientific etc.) you will require additional metadata and there may be a standard specific to your field. Wikipedia provides a useful list on its Metadata Standards page.

2.5.9 Digital preservation

If the life expectancy of your records exceeds that of the technology that holds them then a digital preservation strategy will be required. Electronic records are more at risk of loss and corruption than paper records. Digital information requires active preservation measures.

The main risks to face are:

- Deterioration of the storage medium. Bit-level corruption occurs with fixed and portable hard disks as well as tapes, DVDs and other offline storage. Disks can be corrupted by power cuts and hard drive failures. Tapes deteriorate and have to be replaced after a year or so. CDs and DVDs can become scratched or damaged by light.
- Obsolescence of the hardware or software format. CD/DVD units will soon be as historic as floppy disk drives. Optical disk drives which were supposed to last for 50 years ceased to be supported after around 15 years. File formats may be short-lived and office software may only support backwards compatibility for a few years.

Digital preservation requires a technology watch on hardware and software, regular media refreshes and regular upgrading of software versions.

Documents may require conversion to a format with a longer lifespan. For text documents one of the options is the PDF/A format, which is a constrained form of Adobe PDF version 1.4 but is an open format defined and supported by standard *ISO 19005*. The virtue of PDF/A is that it is device-independent, being self-contained with embedded fonts. The drawbacks are that not all documents will convert to PDF/A and that a PDF/A file is not readily distinguishable from any other PDF file. Since PDF/A-1 was released options have expanded with PDF/A-2 and now we have PDF/A-3, published in 2012, which is based on Adobe PDF 1.7 and allows for embedded documents such as a spreadsheets and CAD files.

The National Archives offers guidance on digital preservation on its digital continuity pages *http://bit.ly/17niOtV* and provides some useful tools such as DROID for identifying and profiling file formats in your organisation.

The Digital Preservation Coalition is another source of useful information and publishes on its website the excellent work by Jones and Beagrie *Preservation management of digital materials: a handbook*[15]

The Open Planets Foundation offers a community hub for digital preservation issues following on from the Preservation and Long-term Access through Networked Services (Planets) project which ran from 2006 to 2010. *www.openplanetsfoundation.org*

ISO 18492:2005 Long term preservation of electronic document-based information[16] provides practical methodological guidance for the long-term preservation and retrieval of authentic electronic document-based information, when the retention period exceeds the expected life of the technology (hardware and software) used to create and maintain the information.

ISO 14721:2012 Space data and information transfer systems—Open archival information system (OAIS) —Reference model[17] is applicable to archives and specifies a reference model for ingesting, managing and presenting information in archive services. It focusses on methods of documenting and managing digital information rather than describing practical preservation techniques.

2.5.10 Additional standards and best practice guidance

In addition to the core documents above there is a wide range of records management guidance on information management pages of The National Archives website *http://www.nationalarchives.gov.uk/information-management/*.

For data protection and information assurance guidance see the Information Commissioner's Office website *www.ico.gov.uk*.

The JISC (Joint Information Services Committee) web site offers guidance for higher education that is often applicable to other sectors on its Infonet pages *www.jiscinfonet.ac.uk*. This includes a classification and retention schedule much of which can apply to all sectors.

The Information and Records Management Society offers members a monthly Bulletin, an annual 2-day conference and several useful resources on its web site *www.irms.org.uk* including a classification scheme and retention schedule for local government.

Public sector web sites often publish policies and procedures which are useful exemplars. Some of the most comprehensive are university web sites such as the University of Edinburgh at *www.ed.ac.uk/schools-departments/records-management-section*.

References

1. ISO 15489:2001 Information and documentation—Records management *www.bsi-global.com*.
2. HM Government Information Principles. December 2011 *http://bit.ly/Zzsb5l*.
3. BSI DISC PD0010 Principles of Good Practice for Information Management. Bill Mayon White and Bernard Dyer *www.bsi-global.com*.
4. ISO 30300:2011 Management Systems for Records *www.bsi-global.com*.
5. ISO 27001 International Standard for Information Security 2005 *www.bsi-global.com*.
6. Data Handling Procedures in Government 2008 *http://bit.ly/ZC72sa*.
7. BS 10008:2008 Evidential weight and legal admissibility of electronic information. Specification and BSI BIP 0008-1:2008 Evidential weight and legal admissibility of information stored electronically *www.bsi-global.com*.
8. Lord Chancellor's Code of practice on the management of records under section 46 of the Freedom of Information Act 2000 *http://bit.ly/11gF5aS*.
9. Records Management Code automated support tool *http://bit.ly/15f3mU3*.
10. Requirements for Electronic Records Management Systems. 2002 revision. The National Archives *http://bit.ly/YuIuB5*.
11. Modular Requirements for Records Systems (MoReq 2010) *www.dlmforum.eu*.
12. ISO 23081-1:2006 Information and documentation-Records management processes-metadata for records-Part 1: Principles *www.bsi-global.com*.
13. ISO 15836:2009 Information and documentation -- The Dublin Core metadata element set *www.bsi-global.com*.
14. E-government Metadata Standard 3.1 2006 *http://bit.ly/11gDD8q*.
15. Jones, M. and Beagrie, N. Preservation management of digital materials: a handbook. Digital Preservation Coalition *www.dpconline.org*.
16. ISO 18492:2005 Long term preservation of electronic document based information *www.bsi-global.com*.
17. ISO 14721:2003. Space data and information transfer systems—Open archival information system—Reference model *www.bsi-global.com*.